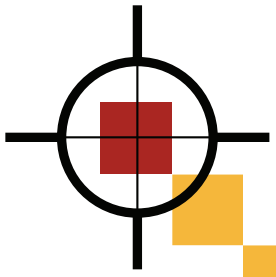
網路安全威脅研究報告



2011 年趨勢

第 17 期

2012 年 4 月出版

Symantec™

Paul Wood
執行編輯
網路安全情報經理
安全機制應變中心

Gerry Egan
產品管理資深主任
安全機制應變中心

Kevin Haley
產品管理部主任
安全機制應變中心

Tuan-Khanh Tran
事業群產品經理
安全機制應變中心

Orla Cox
安全維運部門資深經理
安全機制應變中心

Hon Lau
研發部門經理
安全機制應變中心

Candid Wueest
首席軟體工程師
安全機制應變中心

David McKinney
首席威脅分析師
安全機制應變中心

Tony Millington
軟體副工程師
安全機制應變中心

Benjamin Nahorney
資深資訊開發人員
安全機制應變中心

Joanne Mulcahy
技術產品經理
安全機制應變中心

John Harrison
事業群產品經理
安全機制應變中心

Thomas Parsons
研發部門主任
安全機制應變中心

Andrew Watson
資深軟體工程師
安全機制應變中心

Mathew Nisbet
惡意程式資料分析師
安全機制應變中心

Nicholas Johnston
資深軟體工程師
安全機制應變中心

Bhaskar Krishnappa
資深軟體工程師
安全機制應變中心

Irfan Asrar
安全應變經理
安全機制應變中心

Sean Hittel
首席軟體工程師
安全機制應變中心

Eric Chien
技術主任
安全機制應變中心

Eric Park
資深商業智慧分析師
防垃圾郵件工程部門

Mathew Maniyara
安全應變分析師
防詐騙應變部門

Olivier Thonnard
資深研發工程師
賽門鐵克研究實驗室

Pierre-Antoine Vervier
網路系統工程師
賽門鐵克研究實驗室

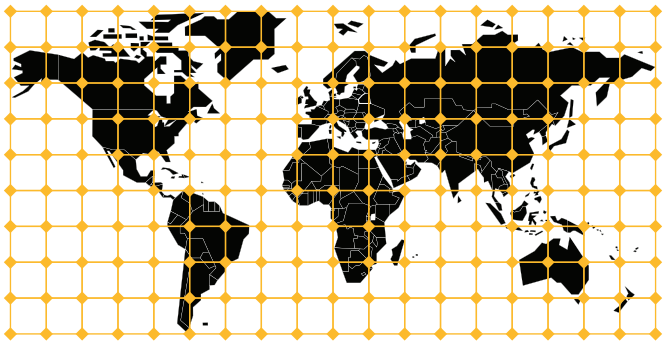
Martin Lee
資深安全分析師
Symantec.cloud

Daren Lewis
首席策略規劃專家
Symantec.cloud

Scott Wallace
資深圖形設計師

目錄

圖表



簡介

賽門鐵克透過「賽門鐵克全球智慧型網路 (Symantec™ Global Intelligence Network)」，建立起世界上最完備的網際網路威脅資料來源，其中包含超過 6,460 萬個攻擊偵測器，每秒記錄數千筆事件。該網路透過賽門鐵克產品與服務的組合 (例如賽門鐵克 DeepSight™ 威脅管理系統、賽門鐵克安全委外管理服務與諾頓消費者產品)，以及其他協力廠商的資料來源，於全球超過 200 個國家及地區監視攻擊活動。

此外，賽門鐵克擁有全球最完善的安全漏洞資料庫，目前已記錄了 47,662 個以上的漏洞 (涵蓋時間長達二十年以上)，其影響範圍包含來自 15,967 多家廠商的 40,006 種產品。

垃圾郵件、網路釣魚、惡意程式等資料的來源非常廣範，包括：擁有 5 百萬個以上誘補帳號的「賽門鐵克探測網路 (Symantec Probe Network)」系統、賽門鐵克雲端服務以及多項其他的賽門鐵克安全技術。賽門鐵克雲端服務的 Skeptic™ 獨家啓發式技術，可在最新及精密的目標式威脅到達客戶網路之前預先偵測並攔截。其 15 個資料中心每天可處理超過 80 億封電子郵件訊息與 14 億以上的網站查詢。此外，賽門鐵克更透過一個由企業、資訊安全廠商及 5 千多萬名一般使用者所組成的大型反詐騙社群來收集網路釣魚資訊。

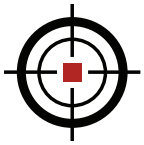
這些資源可賦予賽門鐵克分析師無與倫比的資料來源，進行判別與分析，並提供攻擊、惡意程式碼活動、網路釣魚和垃圾郵件方面最新趨勢的報告評論。而分析的成果就是每年發佈的賽門鐵克網路安全威脅研究報告，它能提供企業用戶與消費者在現在與未來有效保障其系統的重要資訊。

2011 年每月大事記


行動裝置威脅


駭客攻擊


傀儡網路 (BOTNET) 破獲行動


威脅相關資訊


垃圾郵件網路釣魚與 419 詐騙


社交網路

一月


暗藏 Android.Geinimi 後門程式的應用程式現身非官方規範的 Android 市集。


詐騙行動偽裝成印尼 Facebook 應用程式，專門竊取登入帳號密碼。


詐騙者使用巴西 Serrana 水災來詐騙愛心捐款。

二月


資訊安全廠商 HBGary Federal 遭到 Anonymous 駭客團體入侵。


另一個 Android 後門木馬程式 Android.Pjapps 現身非官方規範的 Android 市集。


垃圾郵件作者利用埃及和利比亞的政治動盪發動「419 詐騙」和目標式攻擊。

三月


Microsoft 和美國執法單位破獲 Rustock 傀儡網路。


Android.Rootcager 現身官方的 Android Market。


垃圾郵件作者利用日本地震發動「419 詐騙」、成立假愛心捐款網站、散佈惡意附件檔案。


駭客重新包裝 Google 的 Android. Rootcager 移除工具，在當中挾帶新的 Android.Bgserv 木馬程式。


Comodo Registration Authorities、InstantSSL.it 和 GlobalTrust.it 等憑證核發機構遭駭。出現假的 Google、Hotmail、Yahoo!、Skype 與 Mozilla 憑證。

四月


Sony 發現其 Playstation Network 遭到駭客入侵。在安全性復原之前關閉服務。

伊朗宣稱遭到另一個類似 Stuxnet 的攻擊，叫做「Stars」。

出現會註冊 Facebook 應用程式的惡意程式。

FBI 取得法院命令，關閉 Coreflood 傀儡網路，發送一個「刪除」指令 (該網路內建指令) 到所有受感染的電腦。

垃圾郵件作者與 FakeAV 假防毒軟體販售者趁英國皇家婚禮的機會發動攻擊並進行 SEO 搜尋引擎毒化。

五月

指令碼 (scripting) 攻擊偽造 Facebook 邀請。

賓拉登死訊掀起惡意程式與網路釣魚攻擊。

LulzSec 駭客團體現身，並以「in it for the “LULZ” (為 LULZ 而戰)」為口號。

垃圾郵件作者建立自己的縮短網址服務。

「標籤 (Tagging)」垃圾訊息行動蔓延整個 Facebook 網站。

Facebook 金鑰透過應用程式外流至第三者。

免費版本的熱門 Blackhole 漏洞攻擊工具組釋出/外流。

六月

LulzSec 攻擊 Black & Berg Cybersecurity Consulting，拒絕了先前提供的 $10,000 美元「獎金」。

LulzSec 攻擊美國參議院、中情局 (CIA)、聯邦調查局 (FBI) 等附屬機關，回應美國政府宣布網路攻擊可能被視為戰爭行為的聲明。

「AntiSec 行動」開始，號召駭客攻擊政府網站並公開發現的資料。

LulzSec 發現自己遭到 TeaMp0isoN/th3j35t3r 攻擊，後者認為該團體獲得太多的關注。

虛擬貨幣 Bitcoin 的一項換匯服務遭到駭客入侵。

DigiNotar 憑證核發機構遭駭，導致該公司倒閉。

七月

Microsoft 提供 250,000 美元獎金給提供資訊協助逮捕 Rustock 創辦人之有功者。

艾美懷絲 (Amy Winehouse) 死訊遭受利用來散佈 Infostealer.Bancos 惡意程式。

八月

Trojan.Badminer 現身，將 Bitcoin 採礦運算工作移到繪圖晶片 (GPU) 上執行。

網路釣魚攻擊內含假冒的信任簽章。

九月

垃圾郵件作者利用 911 攻擊事件 10 週年的機會騙取電子郵件地址。

藥物廣告垃圾郵件利用 Delhi 炸彈攻擊事件。

Kelihos 傀儡網路遭 Microsoft 關閉。

十月

W32.Duqu 正式被發現。這很可能就是伊朗在四月時公佈的威脅。

Blackhole 漏洞攻擊工具組發動關於賈伯斯死訊的垃圾郵件行動。

Nitro 攻擊白皮書出爐，詳細說明一項針對化學產業的目標式攻擊。

根據第 11 期 Microsoft Security Intelligence Report (安全性情報報告書)，Java 已成為漏洞攻擊最多的軟體，超過 Adobe 和 Microsoft。

利比亞領袖格達費 (Muammar Gadhafi) 死訊帶來一波散佈惡意程式的垃圾郵件。

Anti-CSRF Token 攻擊現身 Facebook 網站。

十二月

Stratfor 全球事件分析公司遭駭。

垃圾郵件數量掉至三年來的最低點。

2011 年重要數字

55 億

2011 年攔截到的攻擊總數

每日攔截到的網頁攻擊次數

4,595

VS.
2010 年 30 億

620億封
2010 年

420億封
2011 年

每日估計的
全球垃圾
郵件量

每一次資料洩漏
暴露的身分為
110
萬筆

每
299
封垃圾郵件中
有 1 封是
網路釣魚

目標式攻擊

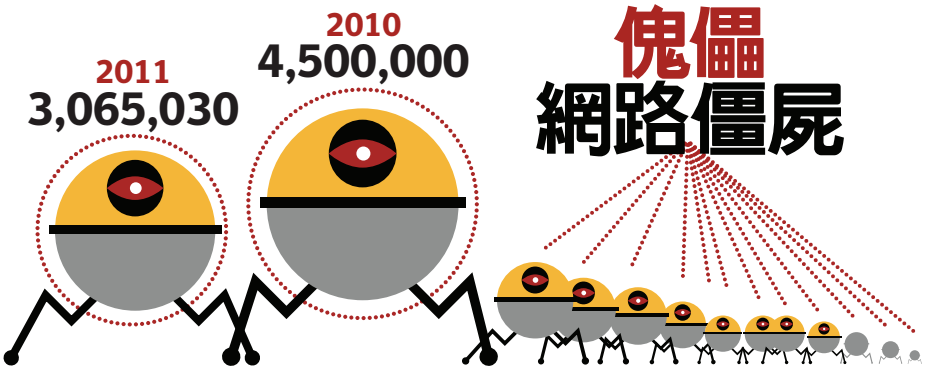
50%
中小企業

18%
小型企業

50%
大型企業

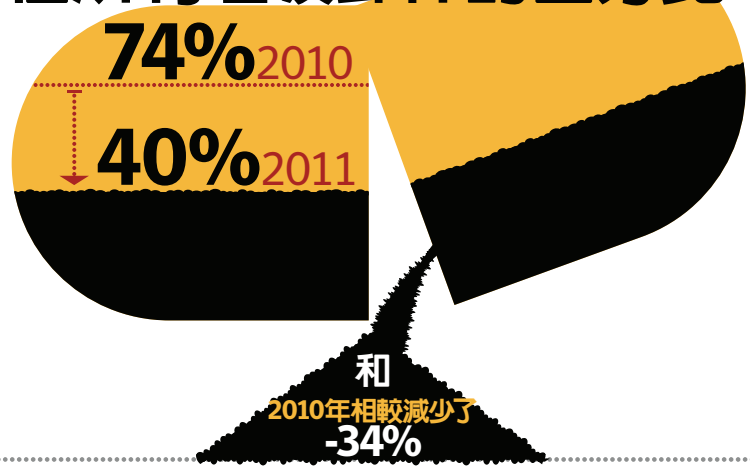
42%
的信箱目標式攻擊鎖定高階主管、資深經理與研發人員

4,989
個全新
漏洞

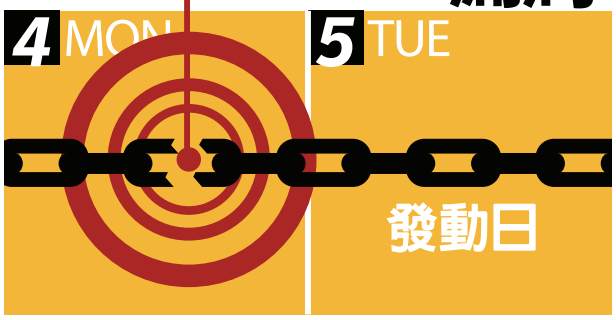


傀儡網路僵屍

藥物垃圾郵件
佔所有垃圾郵件的百分比



8 個全新的零時差漏洞

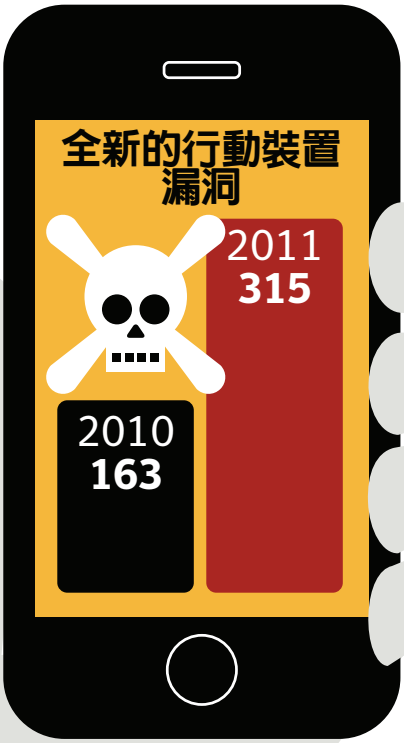


4 億 300 萬種 獨特的 惡意程式變種

VS.

2010 年 2 億 8,600 萬種

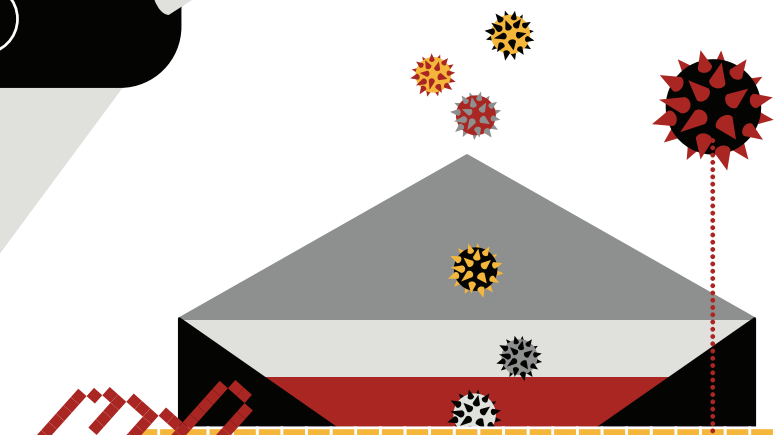
整體 垃圾郵件 比例



55,294 個獨特的惡意網站網域

VS.

2010 年的 42,916 個



每 239 封電子郵件中有 1 封 含有病毒

主管摘要

賽門鐵克在 2011 年攔截了 55 億次惡意攻擊[註1]，比前一年增加了 81%。增加的原因大致上是變形惡意程式攻擊數量爆增的結果，尤其是網頁攻擊工具組與透過電子郵件散佈的社交工程攻擊。其中最危險的就屬利用零時差 (zero-day) 漏洞的目標式攻擊。在目標式攻擊方面，您幾乎不可能知道自己是否已經遭到歹徒鎖定，因為，這些攻擊的特性就是要盡可能規避您的偵測。有別於長期存在的問題，目標式攻擊、政治意圖的駭客攻擊、資料外洩，以及針對憑證核發機構 (Certificate Authorities，簡稱 CA) 的攻擊，都是 2011 年的新聞頭條。回顧這一年，我們發現下列幾項重大趨勢 (大致上依照它們出現在報告正文的順序)：

惡意攻擊爆增 81%

除了攻擊數量爆增 81% 之外，非重複性的惡意程式變種數量也增加了 41%，而且每日攔截到的網頁攻擊數量亦大幅增加 36%。愈來愈多的大範圍攻擊都運用了進階的技巧，例如透過伺服器端變形技術來達到巨大的效果。這項技巧讓攻擊者可針對每一潛在受害者製作一份獨一無二的惡意程式版本。

在此同時，垃圾郵件數量卻大幅下降，而且報告中也顯示新發現的整體漏洞數量出現了負成長 (-20%)。這些數據對照惡意程式成長的趨勢，形成一種有趣的現象。攻擊數量不斷增加，但新的漏洞卻反而減少。不幸的是，在工具組的輔助下，網路罪犯能很有效率地利用現有的漏洞。另一項熱門攻擊散播管道 — 垃圾郵件的數量則減少了，對攻擊的數量並未造成影響。其中的原因之一，就是社交網路已成為另一個廣獲採用的散播管道。在今日，這類網站吸引了數以百萬的使用者，為網路罪犯提供了一個犯罪溫床。由於社交網路的特性使然，使用者會覺得身邊好友環繞，因而感覺不到危險。但很不幸的，情況正好相反，攻擊者正轉移目標，在這類網站上尋找新的受害者。此外，由於社交工程技巧與社交網路傳播迅速的特性，攻擊反而更容易從一位使用者散播到另一位使用者。

網路間諜與商業活動：每一個人都是鎖定攻擊的目標

我們看到進階目標式攻擊在 2011 年有不斷增加的趨勢 (截至 2011 年 11 月底為止，每天平均 94 起)。這份報告資料也顯示，目標式威脅並不僅侷限於攻擊大型企業或企業高階人員。有 50% 的攻擊是針對員工 2,500 人以下的企業，而且有 18% 的攻擊是針對員工不到 250 人的企業。或許，小型企業現在已成為歹徒攻擊大型企業的跳板，因為這些企業有可能是合作夥伴體系的一環，而且防禦相對薄弱。目標式攻擊對所有規模的企業都是一項危險，無人得以倖免。

其攻擊的對象，也已不再侷限於執行長 (CEO) 或資深高階主管。有 58% 的攻擊是鎖定其他的職務，例如：銷售、人事、高階主管助理以及媒體/公關公司。這或許意味著攻擊者已經開始將注意力轉移到更容易得手的目標。如果他們無法攻擊到 CEO 或高階主管，他們或許可以透過企業內的其他連結。值得注意的一點是，這些都是經常需要對外溝通的職務，因此很容易從外部接收到大量的附件檔案。例如：人事部門或人才招募人員都會經常收到並開啓陌生人寄來的履歷或其他附件檔案。

行動電話成為攻擊目標

行動裝置惡意程式的成長，背後需要大規模的使用族群可供攻擊，再加上一些利益的誘因。市場分析機構 Gartner 預估終端用戶智慧型手機的銷售量在 2011 年將達到 4 億 6,150 萬支，並且在 2012 年成長至 6 億 4,500 萬支。在 2011 年，智慧型手機的出貨量將超越個人電腦 (3 億 6,400 萬台)[註2]。而且，儘管個人電腦領域的獲利依然可觀，但行動裝置為網路罪犯提供了獲利潛力更大的全新商機。一張偷來的信用卡最低可能賣到 40-80 美分。但發送高額付費簡訊的惡意程式卻可讓作者每封簡訊收到 $9.99 美元，而且那些不常留意電話帳單的受害者，還可能付了歹徒無數次而不自知。隨著行動裝置的漏洞數量不斷上升 (較 2010 年成長了 93.3%)，惡意程式的作者不僅將現有的惡意程式移植到行動裝置上，他們更開發了行動裝置專屬的惡意程式，目的就是要善用行動裝置所提供的獨特商機，而 2011 年是行動裝置惡意程式首次對企業和消費者造成實質威脅的一年。

此外，行動裝置也為企業帶來了迫切的資料外洩問題。由於行動裝置上參雜了個人資訊和工作資料，因此，機密外洩的問題為企業帶來了真正的風險。而且，有別於桌上型電腦，甚至是筆記型電腦，行動裝置很容易遺失。根據賽門鐵克最近的研究顯示，有 50% 的遺失手機都從未尋回。對於遺失卻缺乏防護的手機來說，96% 的手機資料都將外流。

隨著 SSL 逐漸普遍，憑證核發機構與 Transport Layer Security (TLS) V1.0 通訊協定也成為攻擊目標

SSL (Secure Sockets Layer) 憑證核發機構遭到入侵的知名駭客事件，使得網際網路的信賴支柱受到了威脅。然而，SSL 技術本身並非 DigiNotar 資料外洩事件或類似攻擊當中的脆弱環節，這些事件反倒突顯了整個憑證簽發體系中的機構應該強化自己的基礎架構，並且採用更嚴格的安全程序和政策。TLS 1.0 遭到惡意程式攻擊，突顯出整個 SSL 體系應該升級到更新的 TLS 版本，例如 TLS 1.2 或更高版本。網站經營者都知道應該盡量推廣 SSL 的應用範圍以應付中間人 (Man-In-The-Middle，簡稱 MITM) 攻擊，尤其是一些非交易類的網頁，例如 Facebook、Google、Microsoft 及 Twitter 都開始接納 Always On SSL (全程使用SSL)[註3]。

2 億 3,200 萬個身分遭竊

整體來說，在 2011 年當中共有 2 億 3,240 萬個身分遭到外洩。根據「諾頓網路犯罪索引 (Norton Cybercrime Index)」的分析，儘管駭客攻擊並非資料外洩最常見的原因，但其衝擊卻最大，並且在 2011 年造成 1 億 8,720 萬個身分外洩，是當年所有外洩事件類型當中最多的[註4]。在所有產業當中，導致資料外洩最常見的原因是電腦或其他資料儲存/傳送媒體遭竊或遺失，例如 USB 隨身碟或備份媒體。遭竊或遺失在所有可能導致身分曝光的資料外洩事件當中就佔了 34.3%。

破獲傀儡網路，垃圾郵件大減

2011 年也並非全都是壞消息，垃圾郵件整體數量在該年大幅減少，從 2010 年佔所有郵件的 88.5% 降至 2011 年的 75.1%。原因絕大部分要歸功於執法單位破獲了 Rustock 這個每天散佈大量垃圾郵件的全球化大型傀儡網路。在 2010 年，Rustock 是全球規模最大的垃圾郵件散佈傀儡網路，在該網路消失之後，其競爭對手似乎既無法、也無意願取代其地位。然而在此同時，垃圾郵件作者正逐漸將注意力移轉到社交網路、縮短網址服務以及其他技術，讓垃圾郵件攔截更加困難。

總而言之，這些變化意味著：一方面，數量龐大的非目標式惡意程式與垃圾郵件攻擊數量愈來愈多；另一方面，目標式攻擊、進階持續性威脅，以及針對網際網路基礎架構本身的核心攻擊愈來愈精密。企業應該將這一點牢記在心。因為面對網路罪犯、駭客與間諜的每一次攻擊，企業都必須成功防禦。但歹徒只需一次的僥幸就能得逞。

目標式攻擊使用了客製化惡意程式與更精密的目標式社交工程技巧來取得未獲授權的敏感資訊。這是社交工程演化的未來趨勢，也就是先仔細研究受害者，再針對目標發動攻擊。

守護機密：網路上的產業間諜

2011 年網路間諜活動

目標式攻擊在 2011 年大幅增加，從 2010 年平均每天 77 件上升至 2011 年每天 82 件。此外，由於幾次鬧得沸沸揚揚的事件，進階持續性攻擊威脅 (APT) 也引起更多大眾關注。

目標式攻擊使用了客製化惡意程式與更精密的目標式社交工程技巧來取得未獲授權的敏感資訊。這是社交工程演化的未來趨勢，也就是先仔細研究受害者，再針對目標發動攻擊。一般來說，歹徒會利用目標式攻擊來竊取寶貴資訊 (如客戶資料)，並藉此牟利。對於進階的持續性攻擊威脅來說，目標式攻擊是整個長期間諜行動的一部分，通常會鎖定政府機關和產業當中價值較高的資訊或系統。

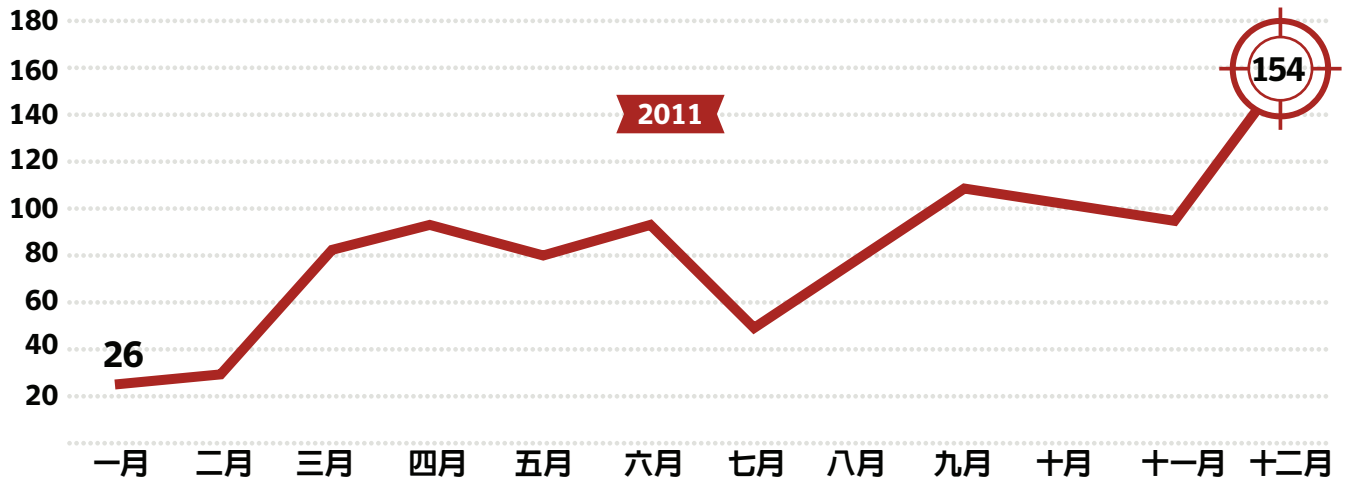
在 2010 年，Stuxnet 的事件登上了新聞頭條。這是一種廣泛散佈的病蟲，但卻含有專門攻擊工業流程監控及控制系統的行為，因而令人懷疑是否專門用來攻擊伊朗的核子設施。它證明了目標式攻擊確實可能在真實世界造成實體的破壞，讓網路間諜的幽靈成真。

Duqu惡意程式在2011 年 10 月現身[註5]。這是 Stuxnet 的後代。它利用零時差 (zero-day) 漏洞來安裝可側錄鍵盤按鍵和其他系統資訊的間諜程式。它預告了類似 Stuxnet 的攻擊即將再起，但至今我們仍未看到任何專門從事網路間諜活動的 Duqu 版本。

2011年也出現了各種針對石油產業、非營利組織 (NGO) 與化學產業[註6]的長期攻擊。Anonymous、LulzSec 與其他團體的駭客主義攻擊在 2011 年佔據了大多數的資訊安全新聞版面。

圖 1

2011 年目標式攻擊趨勢顯示每月發現的平均攻擊數量



資料來源：賽門鐵克雲端服務

進階持續性攻擊威脅

進階持續性攻擊威脅 (APT) 已成為媒體經常使用及誤用的流行名詞，儘管如此，這類攻擊的確是一項真實的危險。例如，2011 年 3 月見報的一項攻擊就造成了一家美國國防外包商的 24,000 多個檔案失竊。而且，這些是檔案該公司正在幫美國國防部 (DOD) 開發的一項武器系統的相關檔案。

政府機構非常嚴肅看待此類威脅。例如，美國國防部已撥出至少 5 億美元的預算來從事網路安全的研究和開發，而英國政府最近也發表了自己的「網路安全策略 (Cyber Security Strategy)」，擘劃了一項總投資高達 6 億 5 千萬英磅的「國家網路安全計劃」(National Cyber Security Programme) 來解決不斷演進的網路威脅，例如：電子犯罪以及國家安全威脅[註7]。

所有進階持續性攻擊威脅都以目標式攻擊為其主要滲透手段，並且利用各式各樣的管道，如順道下載 (drive-by-download)、SQL 溢注、惡意程式、網路釣魚以及垃圾郵件。

APT 與傳統的目標式攻擊有幾項重大差異：

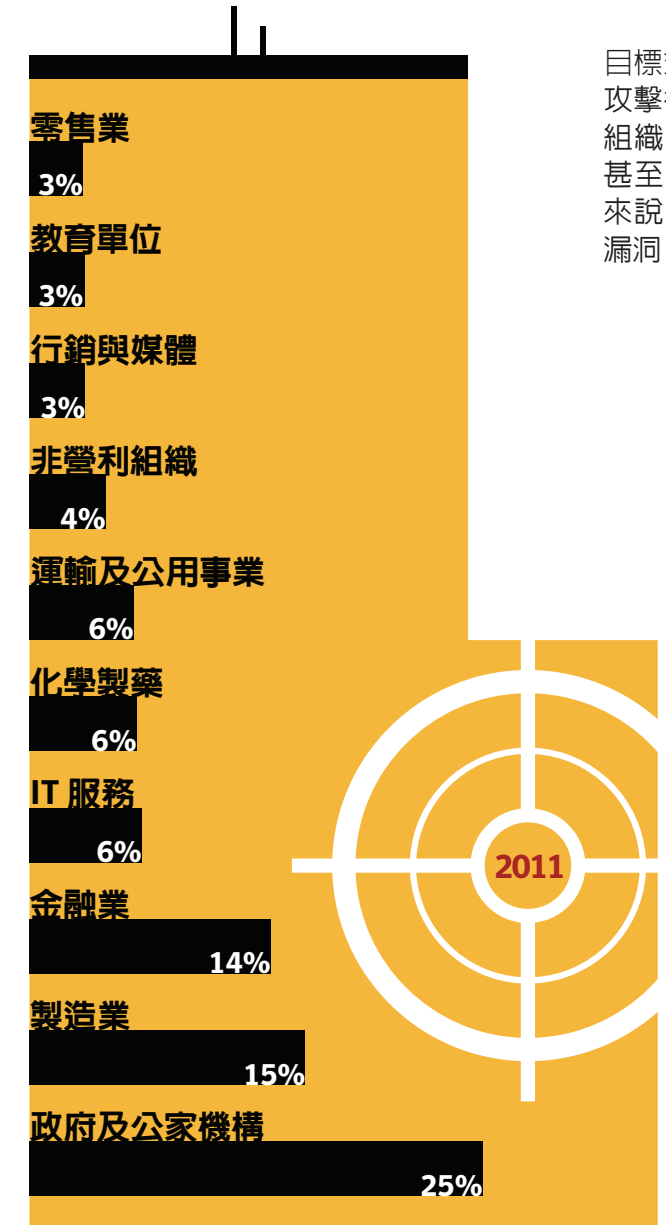
1. 這些攻擊使用的是高度客製化的工具與入侵技巧。
2. 它們通常會使用隱密、耐心且持續滲透的手法來減低被發現的機率。
3. 它們的目標在於獲取高價值、以國家為目標的軍事、政治或經濟情報。
4. 它們有充裕的資金和人員編制，有時是軍方或國家情報單位在背後支持。
5. 他們更可能鎖定一些具策略性的機構，例如：政府機關、國防外包商、知名製造商、關鍵基礎建設營運商及其合作夥伴體系。

圍繞著 APT 的風潮隱藏了一個事實：這些威脅在各種鎖定特定企業組織的攻擊類別中，其實只是特殊案例。由於 APT 持續現身威脅版圖，我們預料其他網路罪犯將從這類攻擊當中學到一些新的技巧。例如，我們已經開始看到大規模惡意程式攻擊利用變形程式碼，也看到垃圾郵件作者在社交網路上使用社交工程技巧。尤有甚者，APT 的目標通常在於竊取智慧財產，這意謂著網路罪犯可能也將在產業間諜活動中，以資訊掮客的全新角色出現。

雖然 APT 影響一般大多數企業的機率相對而言非常低，但很不幸的，您成為目標式攻擊受害者的機會卻相當高。面對 APT 攻擊做好準備的最佳方式就是在整體上確保您擁有抵禦目標式攻擊的良好防護。

圖 2

2011 年目標式電子郵件
攻擊數量排行前十大產業



資料來源：賽門鐵克雲端服務

目標式攻擊

目標式攻擊的影響遍及所有產業。但是，三分之二的攻擊行動都集中在特定產業中的單一或極少數的企業組織，而且半數以上集中在國防與航太產業，有時甚至同時攻擊同一家公司在不同國家的據點。一般來說，這些攻擊每一次行動平均會使用兩種不同的漏洞，有時會使用零時差漏洞攻擊來強化效果。

案例研討

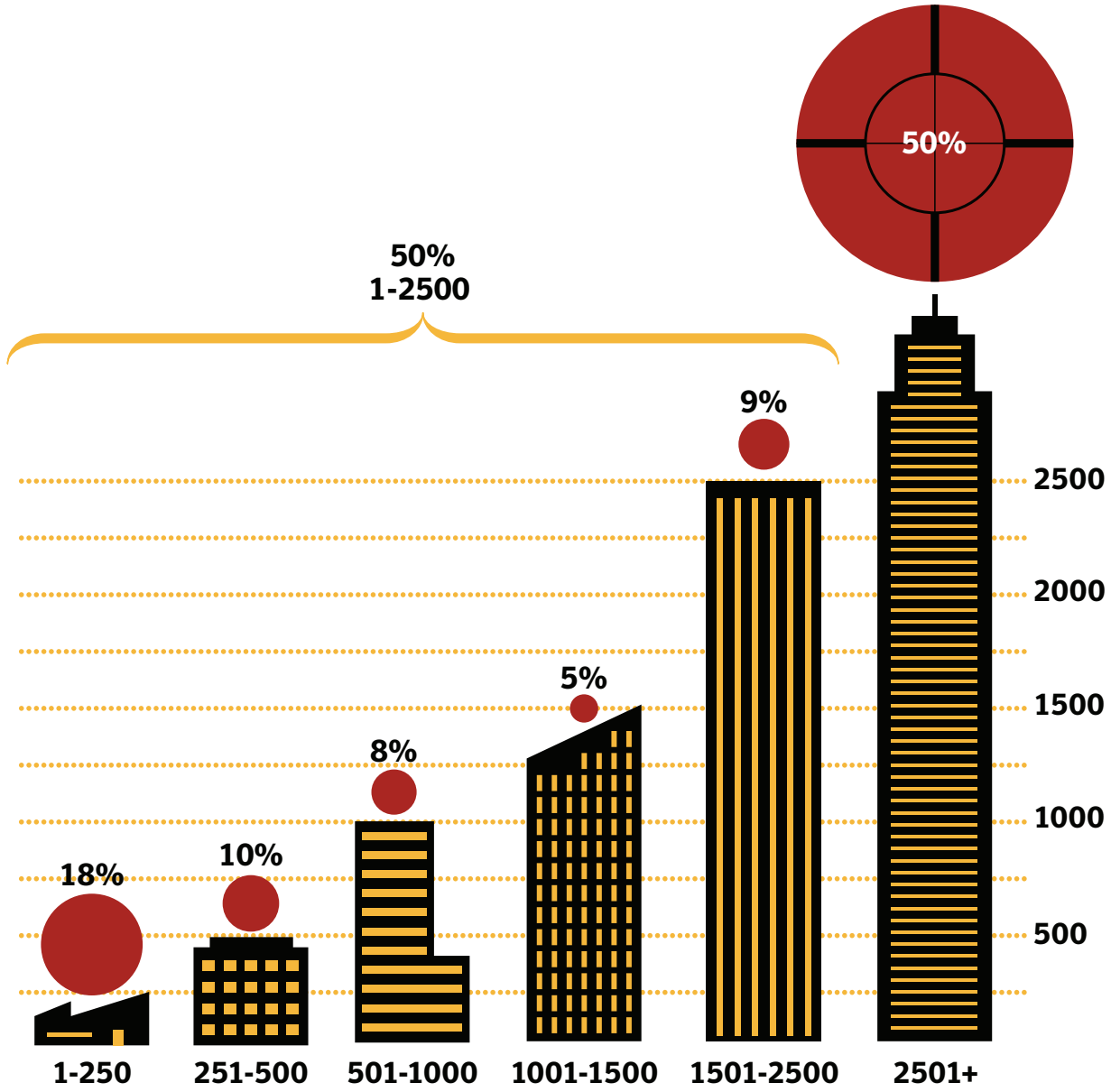
2011 年，我們在化學產業 (及其他產業) 看到 29 家企業遭到假冒已知供應商發出的電子郵件會議邀請。這些電子郵件會在系統上安裝一個知名的後門木馬程式，目的是要竊取寶貴的智慧財產，例如：設計文件和配方。

不過，如果以為只有大型企業才會遭到目標式攻擊那就錯了。事實上，儘管許多小型企業負責人都認為自己不可能成為目標式攻擊的受害者，但這類攻擊卻有一半以上是針對員工人數 2,500 人以下的企業，而且有 17.8% 是針對員工不到 250 人的企業。有可能較小型的企業現在已成為歹徒攻擊較大型企業的墊腳石，因為這些企業有可能是供應鏈或合作夥伴體系的一環，而且防禦相對較弱。

儘管有 42% 的目標式攻擊都鎖定高階主管、資深經理與研發人員，但大多數遭鎖定的人員皆無法直接取得機密資訊。對於攻擊者來說，這類間接攻擊對他們突破嚴密防守的企業來說是很好的敲門磚。例如，其中有 6% 是攻擊人事或人才招募人員，或許是因為這些人員對於收到電子郵件附檔 (如陌生人寄來的履歷) 已習以為常。

圖 3

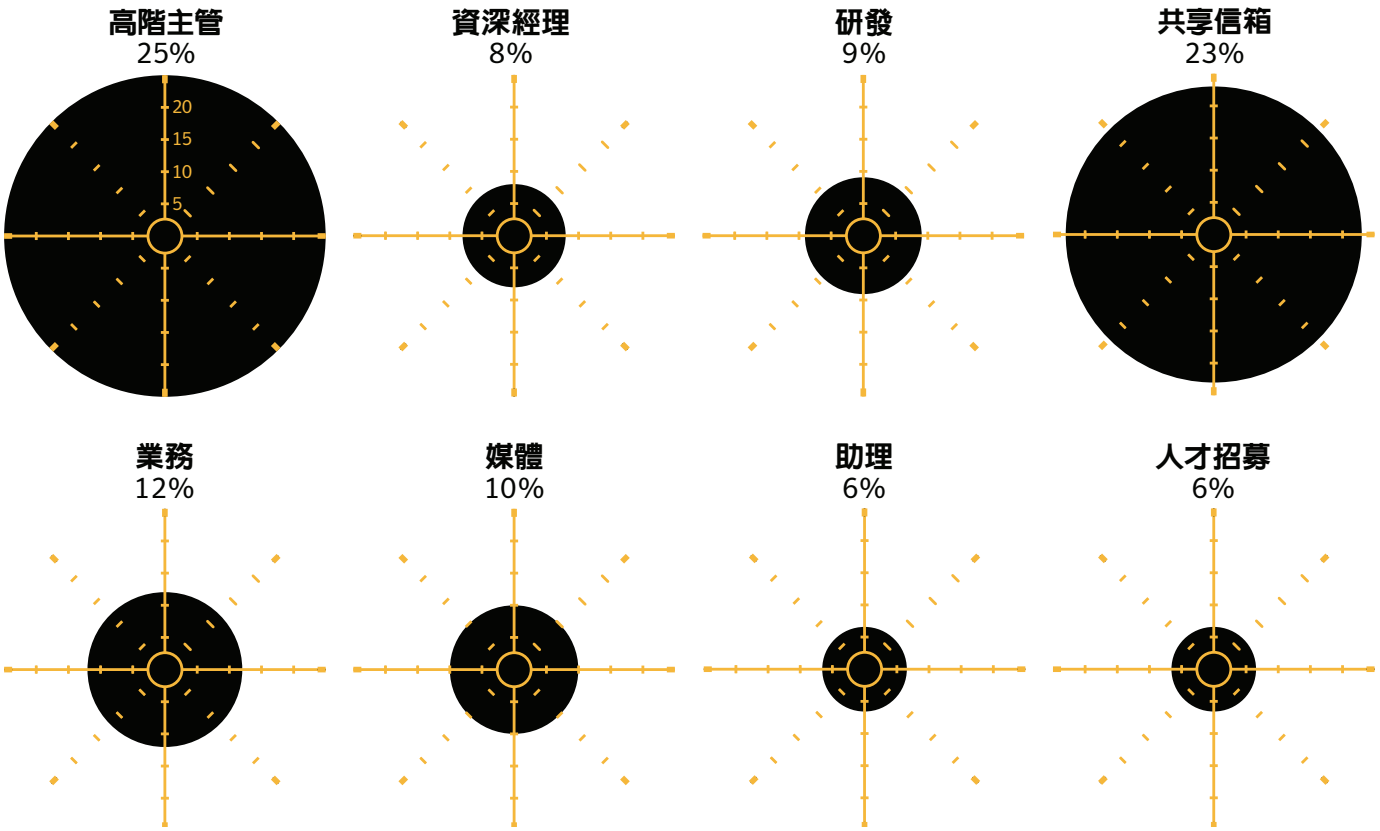
攻擊數量與受害企業規模分布



資料來源：賽門鐵克雲端服務

圖 4

遭鎖定的收件人工作職務分析



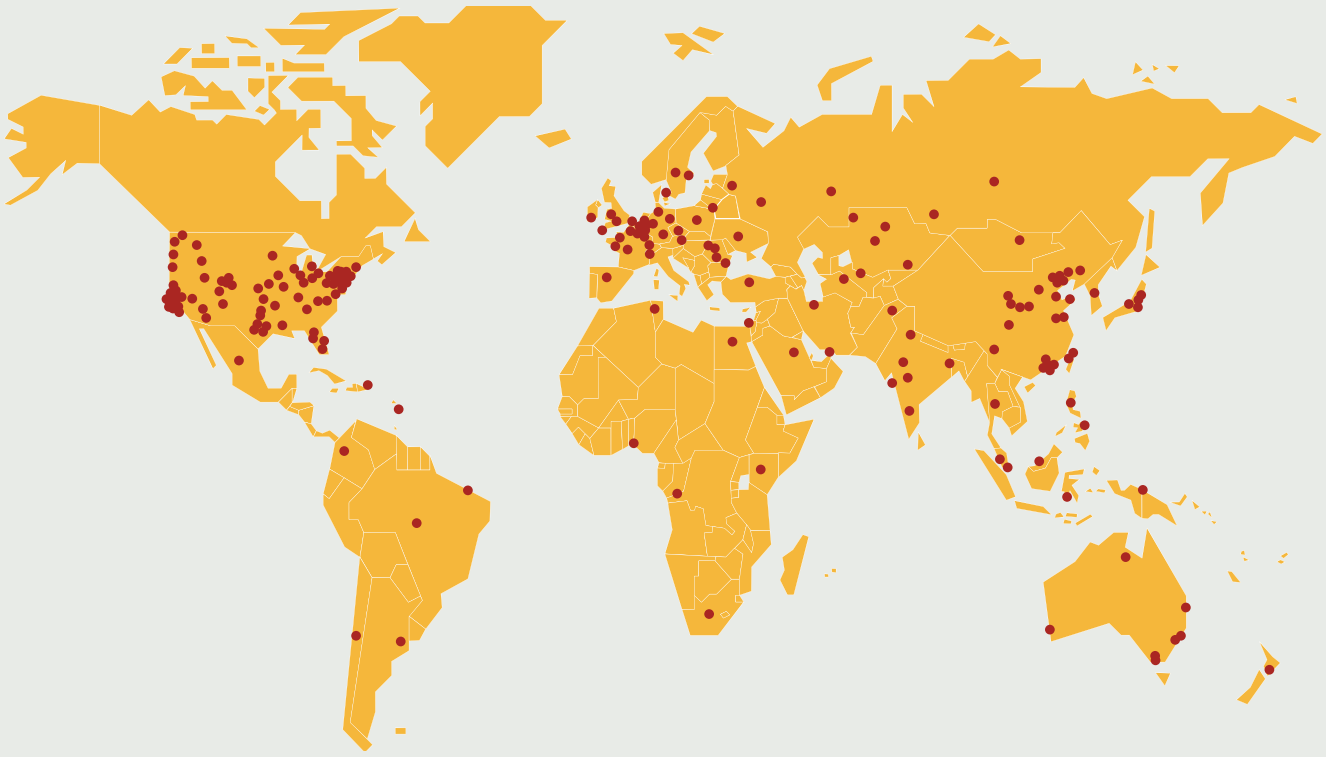
資料來源：賽門鐵克

攻擊來自何處

圖 5 顯示 2011 年所有目標式攻擊來源機器 IP 位址的地理分布。這並不一定是攻擊者所在的位置。

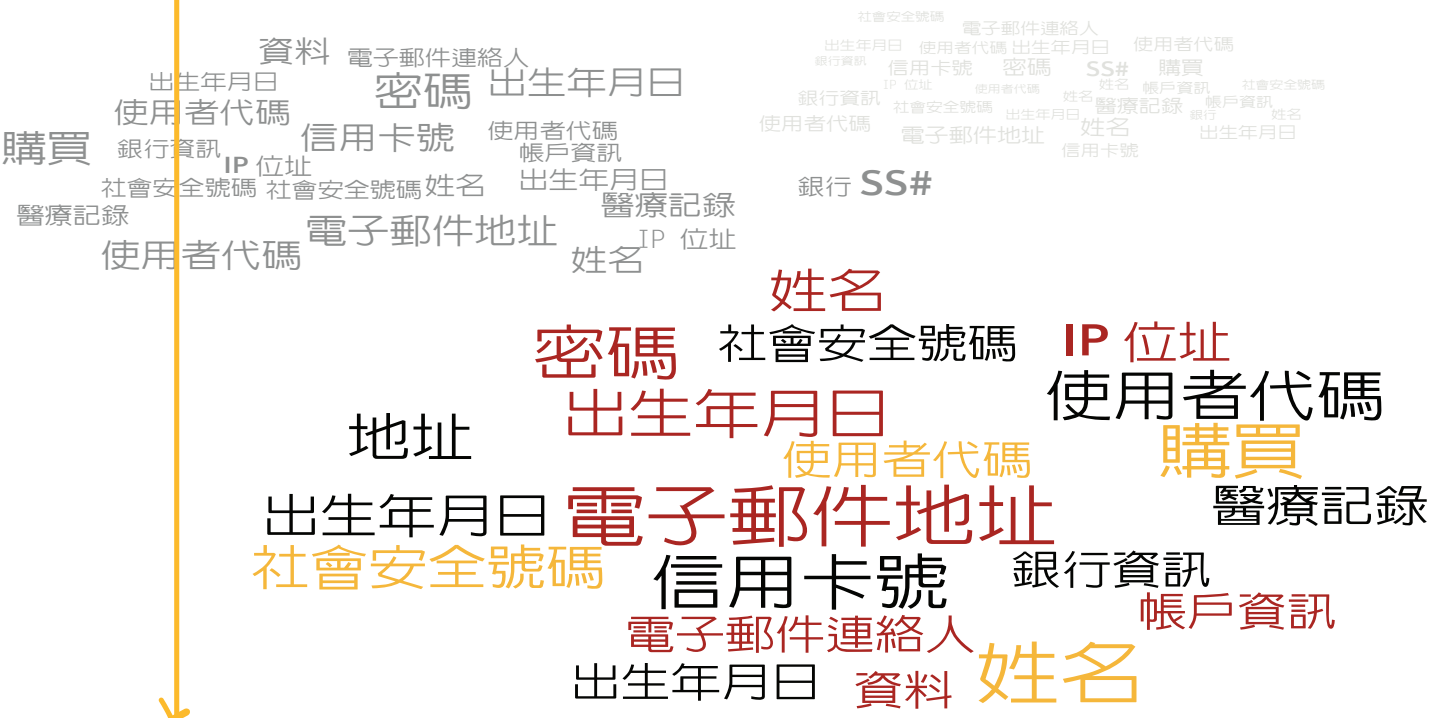
圖 5

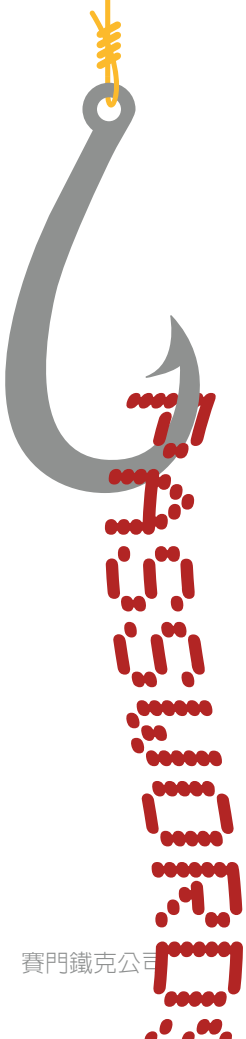
攻擊者 IP 位址所在的地理位置



資料來源：賽門鐵克

儘管這些外洩事件吸引媒體關注，但 2011 年最常見的資料外洩原因卻是傳統的老式竊盜。





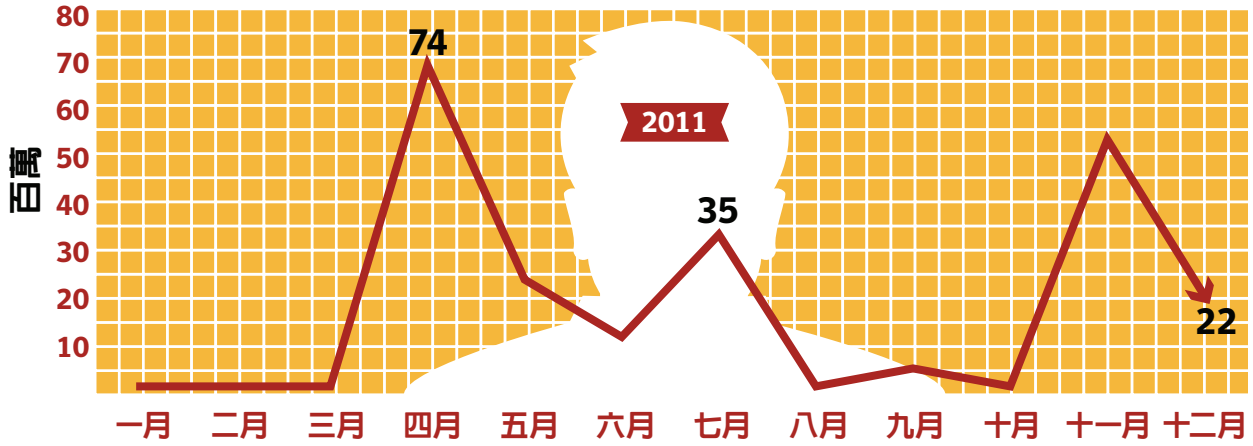
防範資料外洩：捍衛信心及保護資料

政治激進主義和駭客攻擊是 2011 年的兩大威脅主軸，這些威脅將延續到 2012 年。去年，有許多攻擊獲得了不少媒體關注。駭客攻擊可能破壞企業的信心，而個人資料外洩則可能損害企業的信譽。

根據「諾頓網路犯罪索引 (Norton Cybercrime Index)」的分析，儘管駭客攻擊並非資料外洩最常見的原因，但其衝擊卻可能最大，並且在 2011 年造成 1 億 8,720 萬個身分外洩，是當年所有外洩事件類型當中最多的。儘管這些外洩事件吸引媒體關注，但 **2011** 年最常見的資料外洩原因卻是傳統的老式竊盜。

圖 6

資料外洩事件時間序列顯示 2011 年遭到洩漏的身分數量



資料來源：賽門鐵克

2011 年資料外洩

2011是資料外洩之年。根據產業分析報告顯示，電腦軟體、IT與醫療產業就佔了所有失竊身分總數的 **93.0%**。可能的原因是，駭客將某些受害者當成軟性目標，鎖定的是消費性市場，而非資訊安全產業。在所有產業當中，失竊或遺失是最常見的外洩原因，佔 **2011** 年所有外洩身分數量的 **34.3%**，大約 **1,850** 萬個。

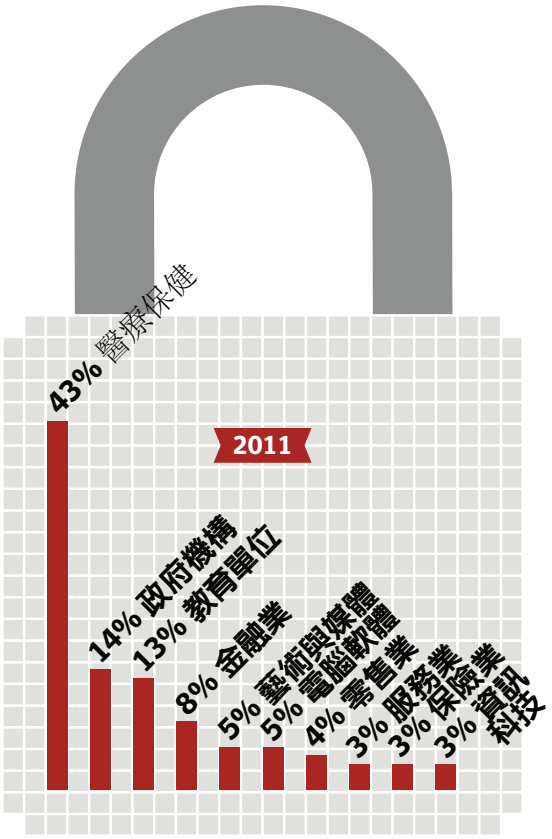
全球來講，平均每次資料外洩事件大約有 110 萬個身分外洩，主要是因為駭客攻擊事件所造成的身分外洩數量龐大。整體來說，在 **2011** 年當中共有 **2** 億 **3,240** 萬個身分遭到外洩。蓄意外洩事件大多鎖定客戶相關資訊，主要是因為可以用於詐騙。

最近賽門鐵克委託 Ponemon Institute 所做的一項調查[註 8]，在研究了英國[註 9]發生的 36 起資料外洩事件之後發現，每人平均成本為 79 英磅，每事件平均總成本為 **175** 萬英磅。同樣地，**Ponemon** 在美國檢視了 **49** 家公司之後發現，資料外洩每人平均成本為 **194** 美元，每事件平均總成本為 **550** 萬美元。呼應前述「諾頓網路犯罪索引 **(Norton Cybercrime Index)**」的資料，**Ponemon** 的研究也發現，疏失 **(**佔英國總案例的 **36%**，佔美國總案例的 **39%)** 與惡意或犯罪攻擊 **(**佔英國總案例的 **31%**，佔美國總案例的 **37%)** 是二大主要原因。

該研究發現，2011 年有更多企業採用了防止資料外洩的技術，因此洩漏的資料數量已減少，客戶流失的現象也比前一年更低。採取一些措施來留住客戶，並且修復受損的信譽與品牌形象，有助於降低資料外洩的成本。

圖 7

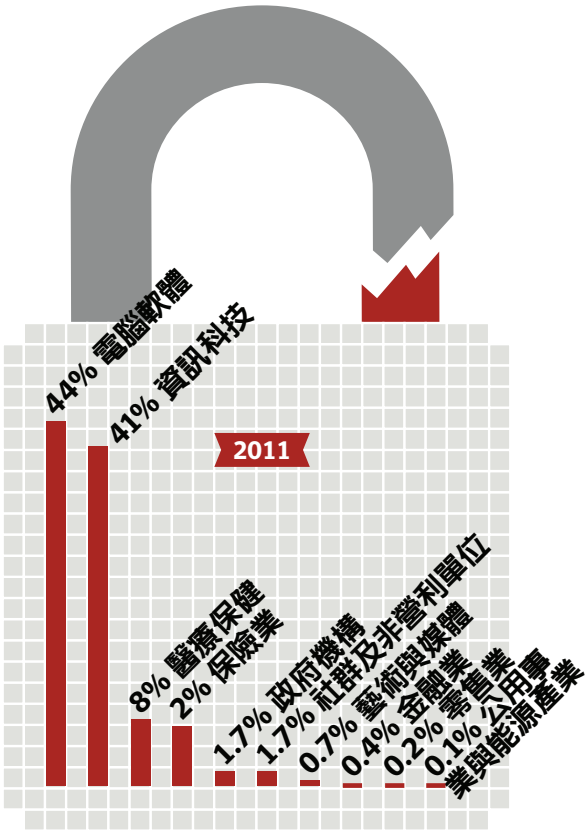
2011 年資料外洩數量排行前十大產業



資料來源：賽門鐵克

圖 8

2011 年身分洩漏數量排行前十大產業



資料來源：賽門鐵克

憑證核發機構成為攻擊目標

憑證核發機構 (Certificate Authorities，簡稱 CA) 是專門核發網站及線上服務加密與驗證所用 SSL 憑證的機構，這些機構在 2011 年遭到前所未有的大量攻擊。

以下是一些與 CA 有關的最知名攻擊案例：

三月

1 某項攻擊破解了資安廠商 Comodo 的某意大利合作夥伴的存取帳號和密碼，並且以該合作夥伴的權限產生了假的 SSL 憑證[註10]。

五月

2 根據報導，Comodo 還有另一家合作廠商也遭駭客入侵，也就是巴西的 ComodoBR[註11]。

六月

3 負責經營 StartSSL 的憑證機構 StartCom 也在六月遭到攻擊未遂[註12]。

4 Diginotar 在六月遭駭。但一開始並未簽發任何憑證[註13]。

七月

5 一項內部稽核發現了 DigiNotar 的內部基礎遭到入侵，並且顯示其加密金鑰遭到了竊取。DigiNotar 遭駭客入侵的結果導致網路上出現了假的 Google、Mozilla 外掛程式和Microsoft Update 憑證，以及其他假憑證[註14]。

八月

6 DigiNotar 遭入侵事件所造成的假憑證已經在網路上流傳。駭客 (外界稱之為 ComodoHacker) 已出面承認主導 Comodo 和 DigiNotar 攻擊，並且宣稱還攻擊了其他憑證核發機構。駭客自稱來自伊朗。

九月

7 網路安全研究人員示範了「瀏覽器 SSL/TLS 漏洞攻擊 (Browser Exploit Against SSL/TLS，簡稱 BEAST)」[註15]，這是一項利用 TLS 1.0 加密技術漏洞的技巧，此加密技術為瀏覽器、伺服器與憑證機構所共同採用的一項標準。

8 GlobalSign 遭到攻擊，儘管憑證金鑰並未外流，其網站伺服器卻遭到入侵[註16]，不過也僅此而已[註17]。ComodoHacker 也出面宣稱策動這次攻擊。

9 荷蘭政府和 DigiNotar 的其他客戶頓時必須撤換所有 DigiNotar 簽發的憑證，因為所有主流瀏覽器都將 DigiNotar 的憑證從其信任的根憑證清單移除[註18]。DigiNotar 因而宣告破產。

十一月

10 Digicert Sdn.Bhd.(Digicert Malaysia) 這個列在 Entrust 之下的中間憑證機構 (與知名的 Digicert Inc. 憑證機構無關)，簽發了一些私密金鑰強度不足的憑證，而且憑證當中缺乏適當的使用期限或撤銷相關資訊。結果，Microsoft、Google 和 Mozilla 都將 Digicert Malaysia 的根憑證從其信任的根憑證清單移除[註19]。這並非攻擊所導致的結果，這是 Digicert Sdn.Bhd. 內部安全控管不佳的結果。

上述攻擊證明，並非所有的憑證核發機構都是一樣的。這些攻擊提高了憑證核發機構的風險，因此，整個產業需要一套一致的高度安全性。對於企業使用者來說，這些攻擊突顯了選擇值得信任、安全可靠的憑證核發機構有多重要。最後，消費者應該隨時使用最新版的瀏覽器，並且應該勤勞一點，檢查一下自己平常瀏覽的網站是否採用值得信任的知名憑證機構所簽發的 SSL 憑證，此外，我們也在這份報告最後提供了一些最佳實務準則的建議。

建立信任和保護最弱環節

奉公守法的使用者都希望建立一個安全、可靠、值得信任的網際網路。根據最新的情勢顯示，一般使用者的信任之戰仍在持續進行當中：

Always On SSL (全程啓用 SSL)。Online Trust Alliance (線上信任聯盟) [註 20] 為 Always On SSL 背書，這是一種讓網站全面建置 SSL 的方法。一些知名網站，如 Facebook [註 21]、Google、PayPal 及 Twitter [註 22] 都已提供了全程使用 SSL 加密及驗證的選項，範圍涵蓋整其服務的所有網頁 **(**而非僅有登入頁面而已**)**。這樣的作法不僅能夠防範 **Firesheep** 之類的中間人 **(man-in-the-middle)** 攻擊 [註 23]，而且可提供端對端的安全性，保護使用者瀏覽的每一個網頁，而非僅有登入畫面或金融交易畫面而已。

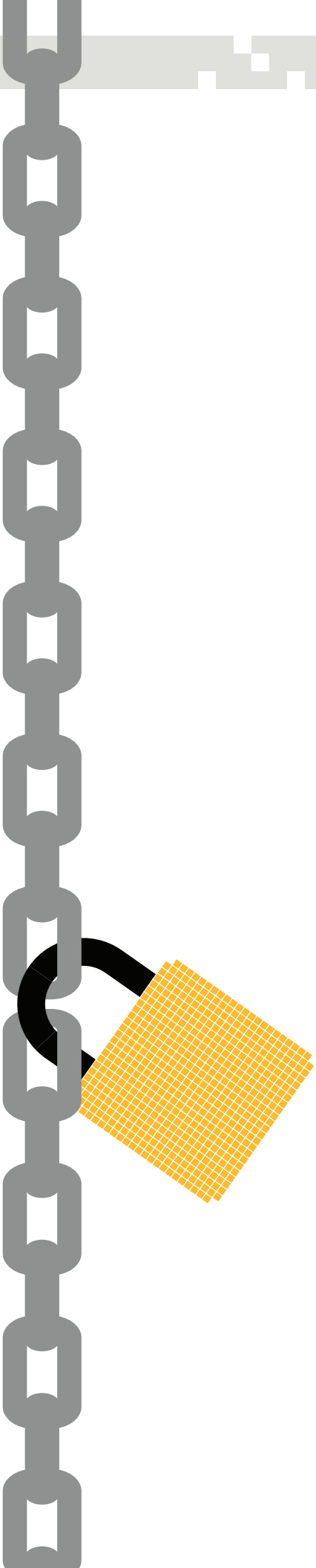
強化驗證的 EV SSL 憑證。EV SSL 憑證提供了最高等級的驗證，因此瀏覽器會以極醒目的方式 (將網址列變成綠色底色) 讓使用者知道自己正在一個安全的網站上。這對防範各式各樣的線上攻擊來說，是一種很有用的防護措施。根據一份賽門鐵克贊助的歐洲、美國及澳洲網際網路購物者消費調查顯示，EV SSL 的綠色網址列有助於提高大多數購物者 (60%) 的安全感 [註 24]。反之，根據一項美國網路消費者研究顯示，當看到瀏覽器發出警告訊息指出網站並未使用安全連線時，90% 的受訪者皆不會繼續進行交易 [註 25]。

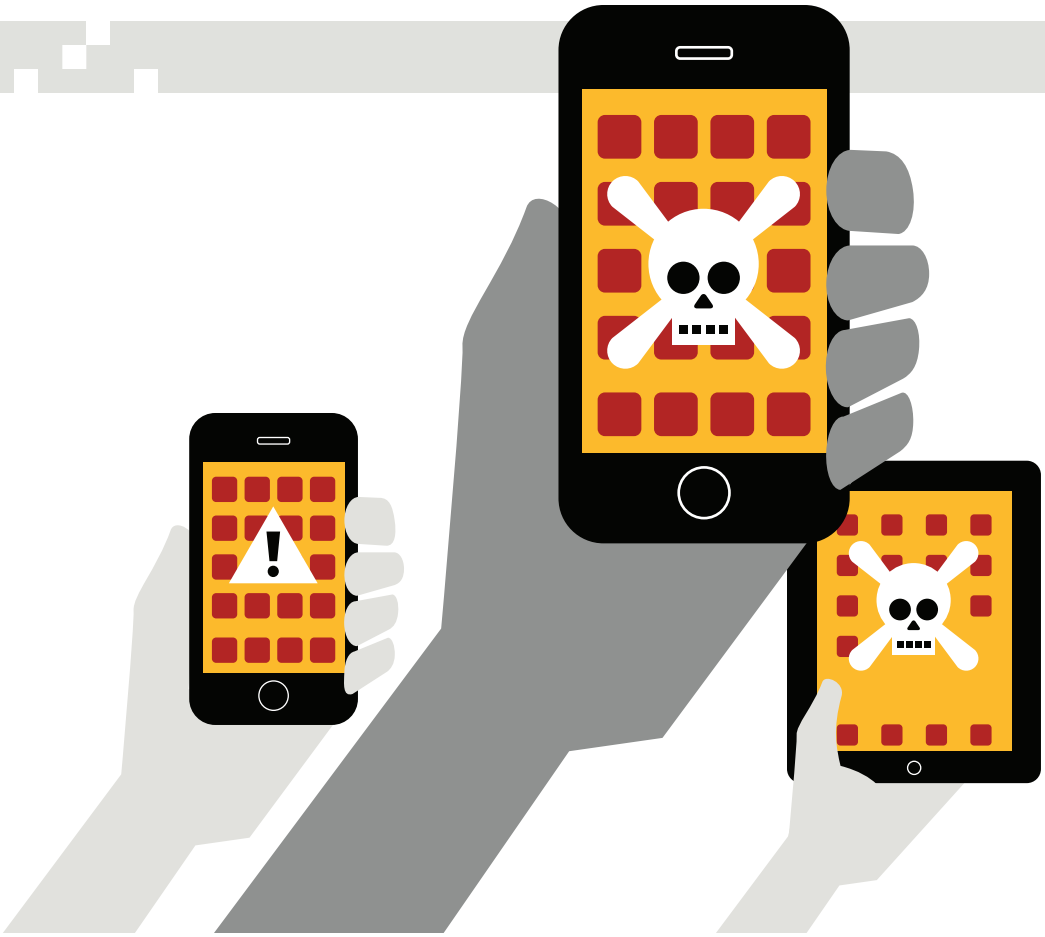
SSL/TLS 憑證的基本要求。CA/Browser Forum (憑證核發機構/瀏覽器論壇) 曾公布一份「具公信力之憑證簽發與管理基本規範 (Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates)」文件，這是第一份針對瀏覽器原生信任之 SSL/TLS 數位憑證核發機構作業的國際基本規範。最新的基本規範已於 2011 年 12 月公告，並且將於 2012 年 7 月 1 日生效。

程式簽署憑證和私密金鑰安全性。一些知名的程式簽署私密金鑰失竊案例突顯出一項事實，那就是持有數位憑證的公司應該妥善照顧並保護自己的私密金鑰 [註 26]。竊取程式簽署金鑰，可讓駭客利用偷來的憑證簽署惡意程式，使得惡意程式偵測難上加難。Stuxnet 和 Duqu 等攻擊正是如此。

DNSSEC (DNS 安全)。這項是一項逐漸被接受的網域名稱系統 **(DNS)** 一致性保護技術。不過，它也並非網路安全的萬靈丹，它無法提供網站身分驗證，亦不提供加密。**DNSSEC** 應該搭配 **Secure Sockets Layer (SSL)** 技術及其他安全機制使用。

法律要求。許多國家，包括歐盟會員國 [註 27] 及美國 **(46** 個州**)** [註 28]，至少都已對特定產業制定了資料外洩通知法，這表示當企業發生資料外洩時，企業必須通知監理機關，必要時還得通知受影響的個人。這些法規不僅對其他立法較不嚴格的地區有鼓舞作用，同時也能確保使用者在資料外洩事件當中迅速接獲通知，並且採取某些行動 (包括修改帳號密碼) 來避免可能的衝擊。





過去十年，我們看到行動裝置數量激增，但行動裝置威脅的成長幅度卻不像個人電腦惡意程式那麼大。

消費化與行動運算：在雲端的風險與效益之間取得平衡

「自備裝置」的風險

愈來愈多的員工開始將自己的智慧型手機、平板電腦或筆記型電腦帶到工作場所使用。此外，許多公司都提供一些額度或補助給員工自行購置電腦設備。這股「自備裝置」的趨勢對於習慣密切掌握網路上所有裝置的 IT 部門來說是一項重大挑戰。此外，員工自備的裝置可能用於非工作相關的活動，反而比純工作用途的裝置暴露在更大的惡意程式風險當中。

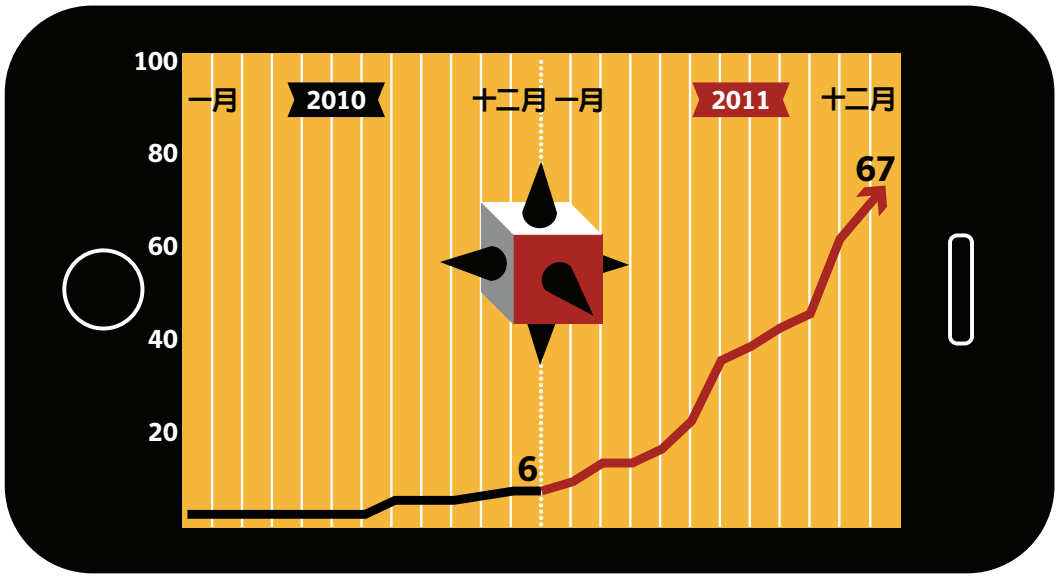
家庭及企業內的行動裝置激增，有很大部分原因是雲端服務和應用程式數量成長所致，少了網際網路連線，很多行動裝置的功能性就大大漸少，失去行動裝置當初的吸引力。

針對行動裝置的威脅

過去十年，我們看到行動裝置數量激增，但行動裝置威脅的成長幅度卻不像個人電腦惡意程式那麼大。仔細回顧個人電腦惡意程式的演進，我們發現行動裝置惡意程式要大幅成長需具備三項條件：一個廣泛的平台、隨手可得的開發工具、充分的誘因 (通常是金錢)。近年來 Android 平台的出現，滿足了第一項條件。2011 年，該平台的市場佔有率不斷成長，呼應了行動裝置威脅的數量成長。

圖 9

2010-2012 年行動裝置惡意程式家族總數量



資料來源：賽門鐵克

有別於蘋果 iPhone 的封閉式系統，Android 平台相對上開放許多。開發人員 (當然也包括惡意程式作者) 較容易為其撰寫和發行應用程式。2011 年，我們看到一些惡意程式家族 (如 Opfake) 從舊式平台移植到 Android 系統。而最新的 Opfake 品種則使用了伺服器端變形技術來躲避傳統的特徵式偵測技術。由於 Android 應用程式並非採用單一官方市集的模式，因此缺乏發行控管，所以，惡意程式作者很容易開發出一些酷似熱門應用程式的木馬程式，儘管 Android 使用者必須明確同意每一個應用程式所要求的權限。

目前，所有的 Android 威脅當中有一半以上不是會收集裝置上的資料就是會追蹤使用者的活動。2011 年所發現的行動裝置威脅當中有將近四分之一會對外發送資料，而手機惡意程式作者最流行的賺錢方式之一，就是利用已感染的手機發送高費率簡訊。2011 年發現的行動裝置威脅當中有 18% 使用這項手法。但愈來愈多的手機惡意程式已不再只是發送簡訊而已。例如，我們已發現會利用 GPS 定位追蹤使用者行蹤並竊取資訊的攻擊。

一個明確而清楚的訊息是：這些威脅的作者不僅更狡猾，而且行為愈來愈大膽。人們將手機視為生活中的個人私人貼身物品，因此能切身感受到手機攻擊的威脅。這類攻擊的動機有時並不一定是金錢：例如，上述案例就是為了收集情報和個人資訊。

行動威脅現在已開始使用伺服器端變形技巧，而行動裝置惡意程式變種數量的成長速度，也比行動裝置惡意程式家族的成長速度還快。賺錢依然是行動裝置惡意程式背後的主要動機，而當今的行動裝置技術情況也提供了一些犯罪機會，只不過還無法達到 Windows 平台可提供的收入規模。

IT 消費化與雲端運算

隨著愈來愈多人將自己的裝置帶到工作場所，消費性科技正逐漸進入辦公室。此外，人們開始也利用社交網站來達成各種目的，例如行銷，同時也透過雲端應用程式，而非公司的內部軟體，來儲存檔案或溝通。

在某些公司，這只是員工「私底下」的個人行為，公司並不支持。但在某些企業，公司則積極擁抱雲端運算及行動辦公室的效益，享受消費性裝置的價格/效能比，藉此降低成本並提高生產力。

例如，全球有 37% 的企業已經開始採用雲端解決方案 [註 29]。

員工在企業內使用雲端服務或個人消費性裝置及消費性網站的行為若缺乏管理，其風險顯而易見。但即使企業積極擁抱這股消費化趨勢，其安全風險依然存在。企業很難在周圍架設滴水不漏的邊界、嚴格管制員工個人的電腦可以安裝些什麼，或是控制資料如何儲存、管理及傳輸，尤其是追蹤企業資料和資訊的使用方式及地點。

二維條碼 (QR Code)

二維條碼這兩年突然在世界各地竄起。人們可以利用智慧型手機上的相機應用程式將這些條碼轉成網址。它既快速又便捷，但卻很危險。垃圾郵件作者正利用它來推銷一些黑市藥品，而惡意程式作者則用它來安裝 Android 手機木馬程式。若再配上縮短網址，使用者基本上很難預先判斷某個二維條碼是否安全，因此，您的二維條碼閱讀器最好會預先檢查網站的信譽再連線至條碼上的網址。

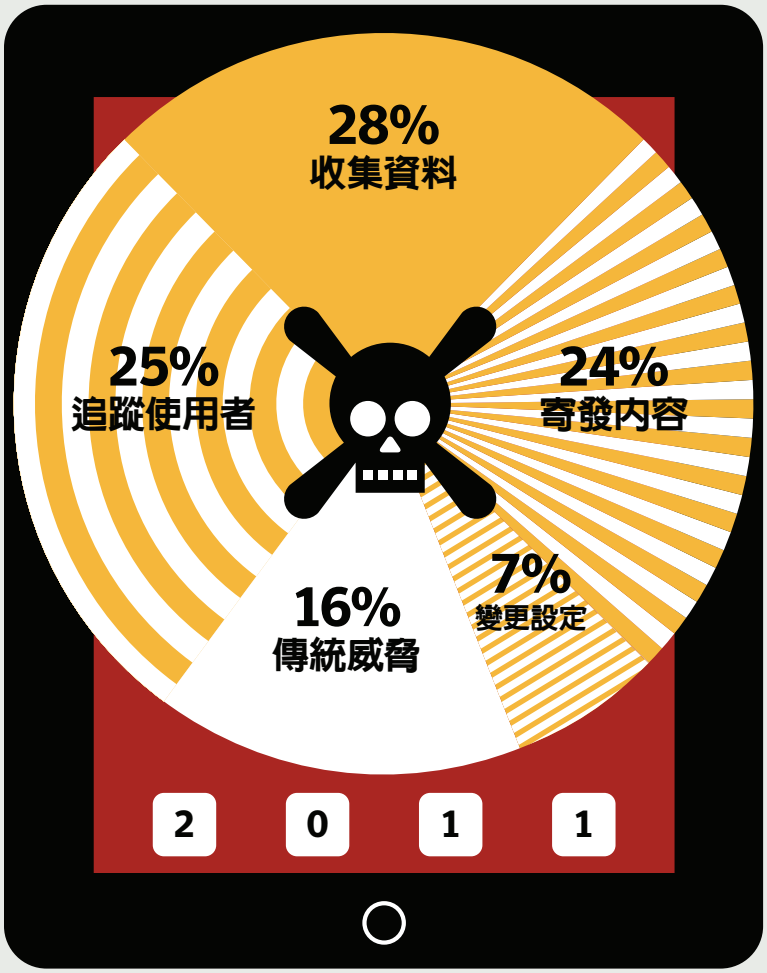
一旦受害者上鉤，歹徒就會開始收線。這類攻擊的下一個步驟就是，誘騙使用者執行某些動作讓威脅得以散佈，例如：安裝某個應用程式、下載所謂的「視訊播放軟體更新」，或者按一下某個按鈕來證明你是人(不是自動化程式)。攻擊者會說服受害者感染自己，並將誘餌散播給社交圈內的每一個人。

我們必須在此聲明，這樣的問題不是 Facebook 才有，所有的社交平台都有這樣的威脅，只是形態稍有不同。這類平台上的威脅數量，與其網站使用者數量成正比，與個別網站的「安全性」或安全程度無關。

行動裝置惡意程式利用您的手機做些什麼

圖 10

行動裝置威脅的主要危害



資料來源：賽門鐵克

許多企業都積極擁抱雲端運算。然而，這並非全無風險。

安心上雲端：在風險之間取得平衡

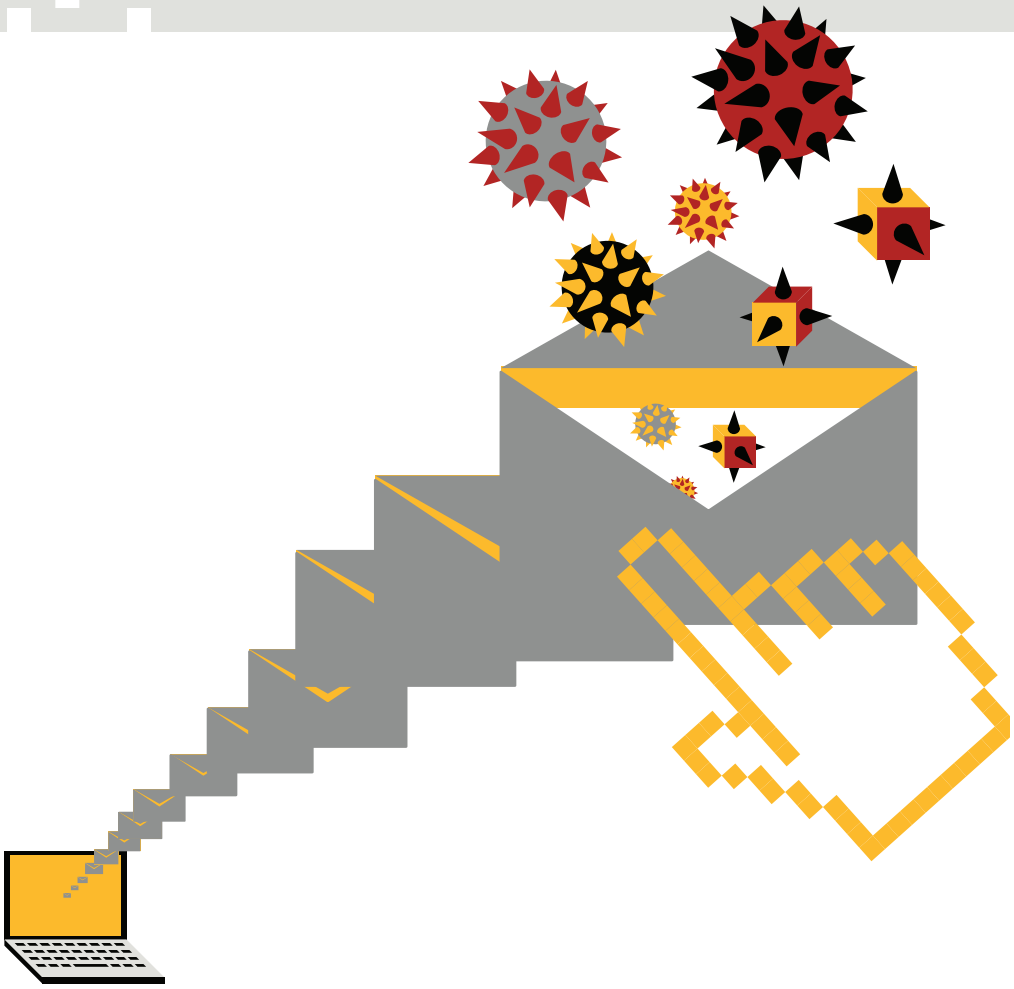
許多企業都積極擁抱雲端運算。它可將一些例行性的服務 (如電子郵件或客戶關係管理) 委外給第三方專業廠商，避免初期的資產投資，取而代之的是更容易預測的每一使用者成本。此外，企業不需辛苦地安裝或升級企業內部硬體，就能享受到更新、更好的技術。

然而，這並非全無風險。第一項風險是對員工使用的雲端服務缺乏管理。例如，員工開始透過檔案分享網站來傳輸大型文件給客戶或供應商，或者在熱門的社交網站上架設非官方公司網頁或論壇。事實上，IT 部門管得愈緊，員工就愈可能透過第三方網站來避開一些限制。

任意使用雲端服務的主要風險包括：

1. 安全與法規遵循 - 使用者、端點裝置與後檯系統之間的介面，都需要具備適當等級的存取控管以確保安全。
2. 資料在網際網路上傳輸時是否加密？
3. 違反資料保護法規 – 例如，如果資料存放在國外，就歐洲的觀點而言，這就可能違反了隱私權法規。
4. 缺乏廠商驗證制度 – 該服務是否信譽優良、安全可靠？必要時，使用者是否可以輕易將資料移轉至其他廠商？
5. 公用和私有雲端業者皆仰賴系統可用性與嚴格的服務等級協議 (Service Level Agreement，簡稱 SLA) 來提升可用性。
6. 儲存在第三方廠商系統上的企業資料如何安全控管。服務廠商是否讓您控制資料的儲存與存取方式？
7. 如果因為任何原因發生服務中斷，企業很可能將無法存取自己的資料。
8. 廠商的條款和條件是否會造成一些法律風險和責任？務必確定廠商的條款和條件是否清楚，以及是否可監控服務效能以達到約定的服務等級協議 (SLA)。

要解決上述問題，IT 主管和 CISO 可制定一份可允許的雲端應用程式清單，就像企業內使用的軟體管制清單一樣。這需要一些適當的使用政策及員工訓練等配套措施，必要時也可使用網站存取控管技術。此外，當員工透過一些消費性網站來從事商業行為時，例如使用社交網路來行銷，企業必須保護使用者，防止透過網站散佈的惡意程式和垃圾訊息等潛在攻擊。



網路釣魚電子郵件的比例隨企業規模大小而有很大差異，最小和最大的企業最容易吸引這類郵件，但垃圾郵件的比例則各規模的企業幾乎都一樣。

垃圾郵件活動趨勢

2011 年垃圾郵件

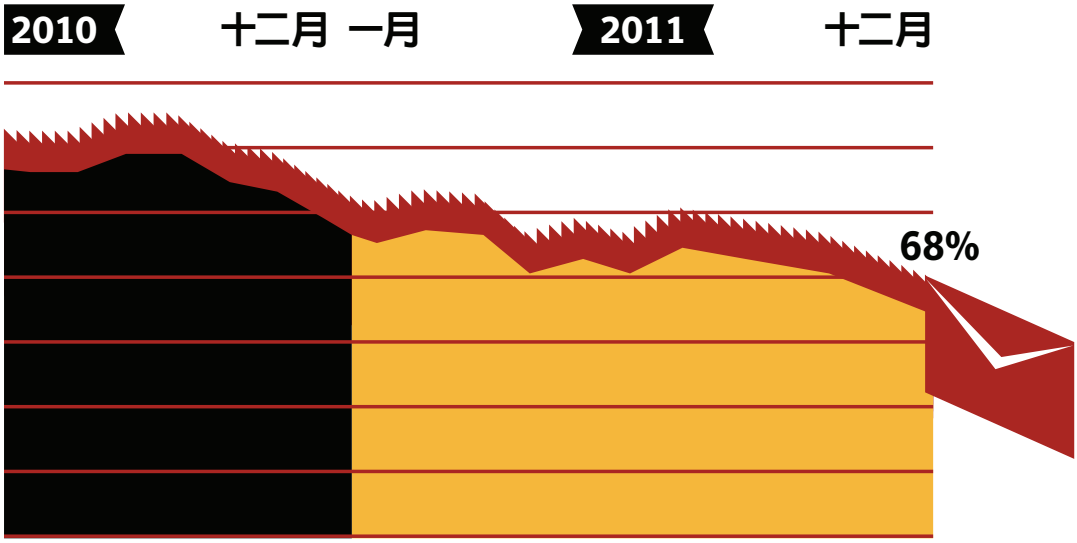
儘管垃圾電子郵件數量在 2011 年大幅減少 (從 2010 年平均佔總郵件數量的 88.5% 降至 2011 年的 75.1%)，但垃圾郵件依然是許多企業長久以來的痼疾，而且是小型企業的無聲殺手，特別是電子郵件伺服器每天塞滿數百萬封垃圾郵件的小型企業。藉由傀儡網路的力量 (也就是遭惡意程式感染，受到網路罪犯控制的電腦網路) ，垃圾郵件作者每天都能散發數十億封的垃圾郵件，不僅阻塞企業網路，更會拖慢通訊速度。2011 年全球每天流通的垃圾郵件數量平均約 420 億封，相較於 2010 年則為 616 億封。

2011 年，垃圾郵件、網路釣魚和「419 詐騙」利用了各種政治事件 (如「Arab Spring 阿拉伯之春」)、公眾人物死訊 (如：格達費、賈伯斯、艾美懷絲) 以及天災 (如日本海嘯)。它們利用這些事件的原因，就和報紙以頭版報導這些事件的原因一樣：吸引讀者的注意力。

有別於垃圾郵件，網路釣魚活動數量持續上升 (2011 年最高達 0.33%，也就是每 298.0 封電子郵件就有一封；2010 年則為 0.23%，也就是每 442.1 封就有一封)。網路釣魚電子郵件的比例隨企業規模大小而有很大差異，最小和最大的企業最容易吸引這類郵件，但垃圾郵件的比例則各規模的企業幾乎都一樣。

圖 11

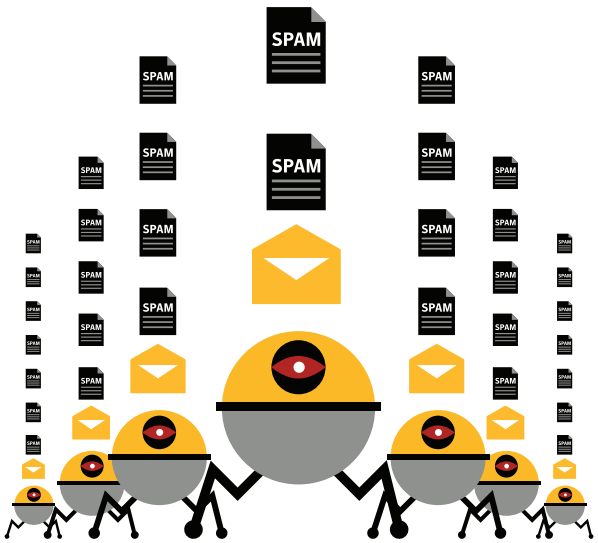
2011 年垃圾郵件的比例



資料來源：賽門鐵克

傀儡網路對垃圾郵件的影響

整體來說，2011 年全球流通的所有垃圾郵件當中約有 81.2% 是由傀儡網路所製造的，2010 年則為 88.2%。在 2011 年 3 月 16 日至 17 日之間，許多位於美國境內的 Rustock 指令與控制伺服器 (C&C) 遭到美國聯邦執法單位查獲並關閉，導致全球垃圾郵件數量急劇下滑，從查獲前一週的每天 510 億封下降至查獲後一週的每天 317 億封。



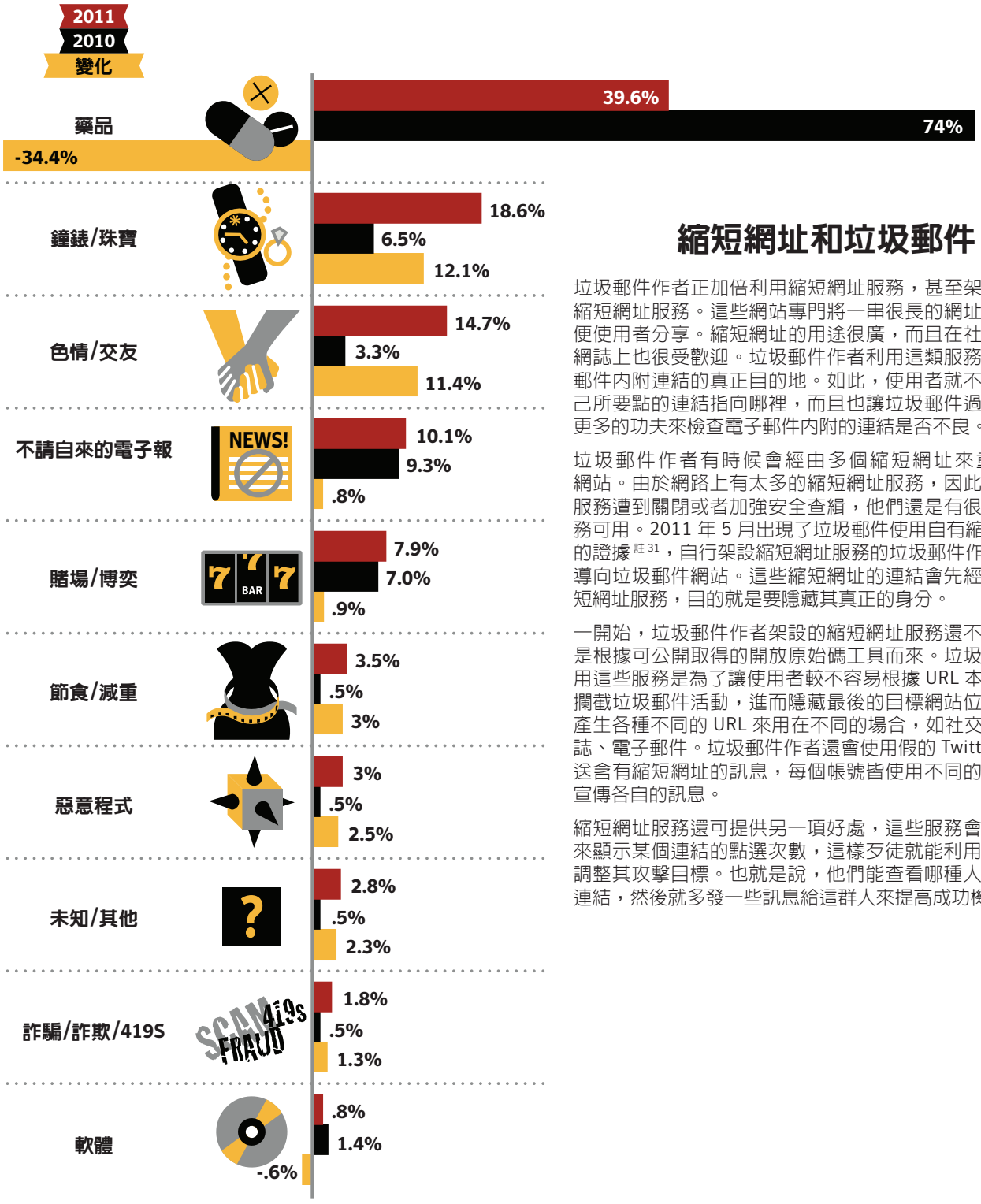
樣貌不斷改變的垃圾郵件

2010 年與 2011 年之間，藥品廣告的垃圾郵件減少了 34%，絕大部分原因是 Rustock 傀儡網路遭到查獲所致，因為該網路主要就是散佈有關藥品廣告的垃圾郵件。反觀鐘錶、珠寶及色情/交友相關的郵件所佔的比例卻因而上升。不僅流通的垃圾電子郵件數量變少了，訊息也變小了，而且英文成為垃圾郵件最通用的語言 [註 30]，其次是葡萄牙文、俄羅斯文和荷蘭文 (只不過它們的「市佔率」小得多)。

隨著社交網路與微網誌網站持續成長，除了傳統的電子郵件之外，垃圾郵件作者也開始轉而攻擊這類目標 。讓訊息不斷轉貼，不單只是行銷人員的夢想而已，專門散佈惡意程式和垃圾郵件的網路罪犯，也在不斷尋找方法來利用社交媒體的廣大力量，誘騙使用者幫他們散佈惡意連結。

圖 12

2010-2011 年十大垃圾電子郵件類別



資料來源：賽門鐵克雲端服務

縮短網址和垃圾郵件

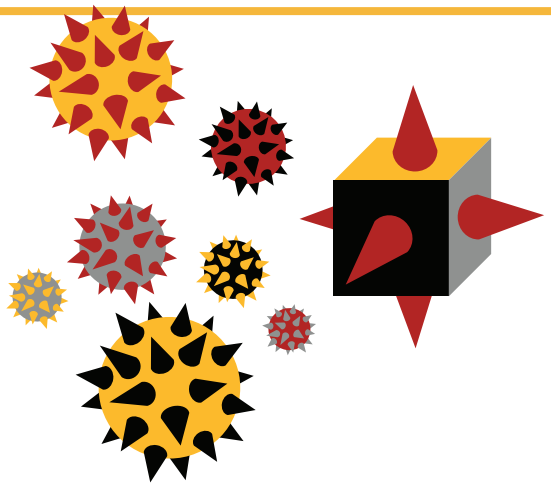
垃圾郵件作者正加倍利用縮短網址服務，甚至架設起自己的縮短網址服務。這些網站專門將一串很長的網址縮短，以方便使用者分享。縮短網址的用途很廣，而且在社交網站和微網誌上也很受歡迎。垃圾郵件作者利用這類服務來隱藏垃圾郵件內附連結的真正目的地。如此，使用者就不容易判斷自己所要點的連結指向哪裡，而且也讓垃圾郵件過濾軟體要花更多的功夫來檢查電子郵件內附的連結是否不良。

垃圾郵件作者有時候會經由多個縮短網址來重導至某個網站。由於網路上有太多的縮短網址服務，因此，就算某個服務遭到關閉或者加強安全查緝，他們還是有很多其他的服務可用。2011 年 5 月出現了垃圾郵件使用自有縮短網址服務的證據[註 31]，自行架設縮短網址服務的垃圾郵件作者將瀏覽者導向垃圾郵件網站。這些縮短網址的連結會先經過正派的縮短網址服務，目的就是要隱藏其真正的身分。

一開始，垃圾郵件作者架設的縮短網址服務還不成熟，而且是根據可公開取得的開放原始碼工具而來。垃圾郵件作者使用這些服務是為了讓使用者較不容易根據 URL 本身來偵測並攔截垃圾郵件活動，進而隱藏最後的目標網站位置。他們會產生各種不同的 URL 來用在不同的場合，如社交網站、微網誌、電子郵件。垃圾郵件作者還會使用假的 Twitter 帳號來發送含有縮短網址的訊息，每個帳號皆使用不同的熱門主題來宣傳各自的訊息。

縮短網址服務還可提供另一項好處，這些服務會提供儀表板來顯示某個連結的點選次數，這樣歹徒就能利用這項資訊來調整其攻擊目標。也就是說，他們能查看哪種人比較會點選連結，然後就多發一些訊息給這群人來提高成功機率。

賽門鐵克的雲端式技術與信譽系統，還能協助偵測並攔截從未出現過的全新及新興攻擊，例如：利用未知零時差 (zero-day) 漏洞的目標式攻擊。



惡意程式碼趨勢

2011 年惡意程式

藉由惡意程式碼的分析，我們能夠判斷目前熱門的威脅類型與攻擊管道。端點裝置通常是最後一道防線，但對於專門透過 USB 儲存裝置、不安全的網路連線以及遭到入侵/感染的網站所散佈的攻擊來說，端點裝置通常是第一道防線。賽門鐵克的雲端式技術與信譽系統，還能協助偵測並攔截從未出現過的全新及新興攻擊，例如：利用未知零時差 (zero-day) 漏洞的目標式攻擊。在雲端及端點裝置上分析惡意程式活動趨勢，能有助於發掘企業所面臨的威脅特性，尤其是混合式攻擊及行動工作者所面對的威脅。

由於網際網路人口龐大，美國、中國和印度依然是整體惡意活動的三大來源。來自美國的整體平均攻擊比例，比 **2010** 年上升了 **1** 個百分點，而中國所佔的比例卻比 **2010** 年下降了約 **10** 個百分點。

美國是所有惡意活動的首要來源 (除了惡意程式碼與垃圾郵件殭屍之外，這二項由印度領先)。來自美國的傀儡電腦活動大約佔 **12.6%**，網頁式攻擊佔 **33.5%**、網路攻擊站 **16.7%**、網路釣魚網站佔 **48.5%**。

網站惡意程式

順道攻擊 (drive-by attack) 依舊是消費者與企業所面臨的一項挑戰。這類攻擊在每年的嘗試感染攻擊當中佔了數億次之多。這是當使用者造訪某個專門散佈惡意程式的網站所遭到的攻擊。發生的時機包括使用者點選了某個電子郵件當中或來自社交網站的連結，或者瀏覽了某個遭到感染的正常網站。

攻擊者會不斷變換手法，而且已相當老練。那些拼錯字、不夠真實的電子郵件已經過時，取而代之的是「點按挾持 (clickjacking)」或「按讚挾持 (likejacking)」手法，例如當使用者造訪某個網站來觀賞一個吸引人的影片時，攻擊者就利用這個點按的動作在使用者的 Facebook 好友塗鴉牆上張貼回應，藉此引誘這些好友點選同樣的惡意連結。

為此，Facebook 特別設置了一套「點按挾持網域信譽系統 (Clickjacking Domain Reputation System)」來消除大量的點按挾持攻擊，這套系統會在使用者按「讚」時查看其網域是否可能有問題，若是則再詢問使用者一次來確認，確認之後才會張貼訊息。

根據專門掃描網頁以尋找惡意程式散播網站的「諾頓網頁安全 (Norton Safe Web)」[註 32] 服務的資料，大約有 61% 的惡意網站其實是遭到入侵並感染了惡意程式碼的正常網站。

最常遭到感染的網站前 5 大類別排行：

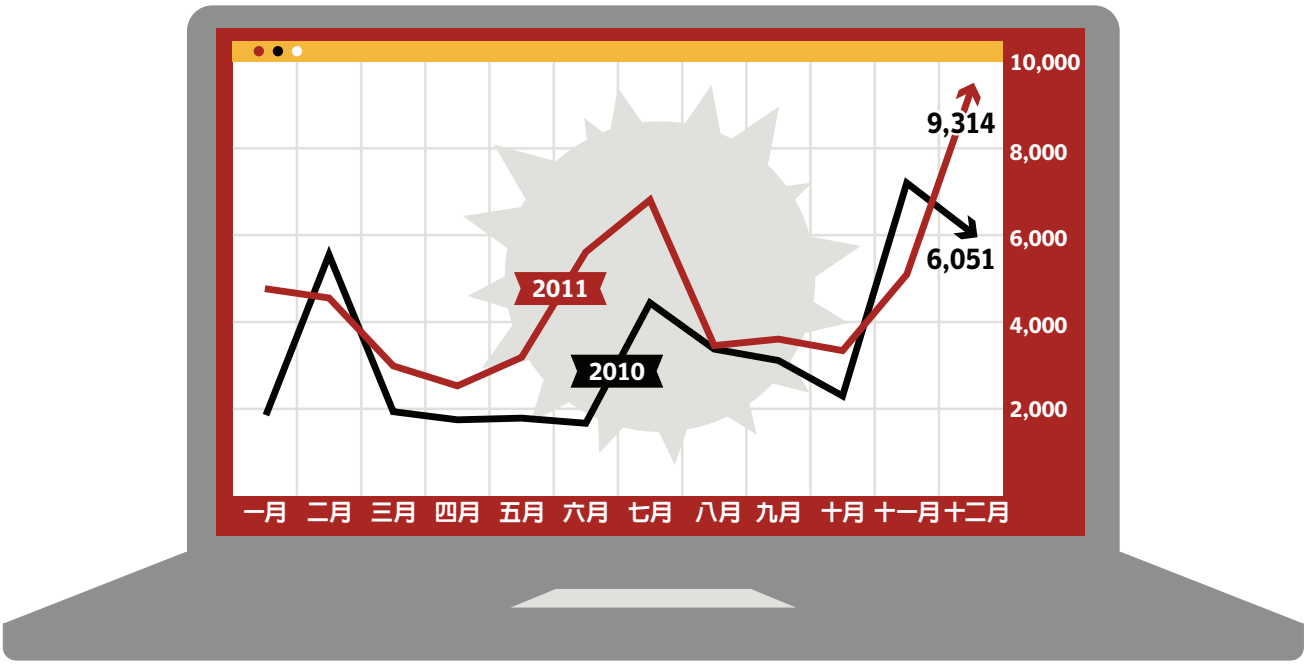
1. 部落格/網頁通訊
2. 託管/個人託管網站
3. 商業/經濟
4. 購物
5. 教育及參考

有趣的是，專門提供成人/色情內容的網站，並不在前 5 名之內，反而在第 10 名。完整的排名請看圖 16。

此外，宗教和意識形態網站，其每一網站平均感染的威脅數量竟然是成人/色情網站的三倍。我們的推測是，色情網站要靠網際網路賺錢，因此得維持其網站不受惡意程式感染才行，畢竟惡意程式不利客戶上門。

圖 13

2011 年平均每天發現的惡意網站數量



資料來源：賽門鐵克雲端服務

在 2011 年，賽門鐵克的 VeriSign 網站惡意程式掃描服務[註 33] 掃描了超過 82 億個 URL 是否有惡意程式感染，結果發現大約每 156 個非重複的網站就有 1 個含有惡意程式。含有漏洞的網站較容易遭到惡意程式感染，而且，從 2011 年 10 月開始，賽門鐵克開始為其 SSL 客戶提供網站漏洞評估掃描服務。從該年的 10 月至年底為止，賽門鐵克發現 35.8% 的網站至少有一個漏洞，而且 25.3% 至少有一個嚴重的漏洞。

透過電子郵件散佈的惡意程式

惡意電子郵件佔電子郵件總量的佔比例在 2011 年有所增加。大型企業的成長幅度最大，員工人數超過 2,500 人的企業每 205.1 封電子郵件就有 1 封是惡意電子郵件。至於員工不超過 250 人的中小企業，每 267.9 封電子郵件就有一封是惡意電子郵件。

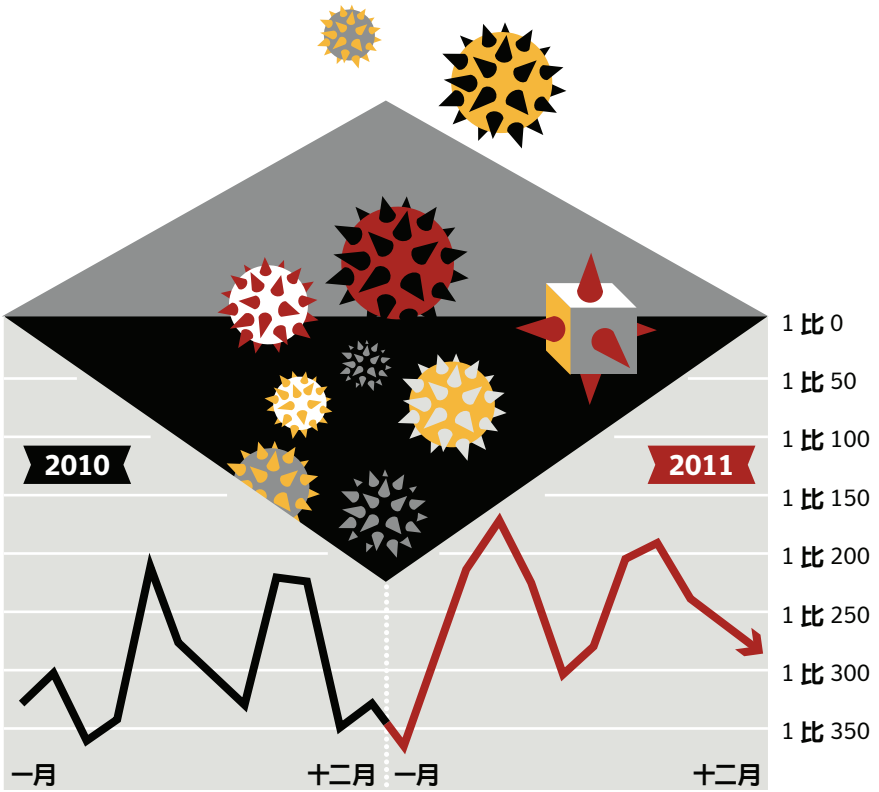
歹徒使用了各種類型的附件來偽裝其惡意程式，例如：PDF 檔案和 Microsoft Office 文件。許多這類資料附件檔案內含了一些專門利用其應用程式漏洞的惡意程式碼，而且至少有二項攻擊使用了 Adobe Reader 的零時差 (zero-day) 漏洞。

惡意程式作者使用社交工程技巧來誘騙受害者點選感染的附件檔案。例如，近期的攻擊就假冒來自知名快遞服務的無法投遞訊息。還有另一個例子是假冒網路連接的掃描器和影印機發出的掃描完成影像電子郵件。很不幸地，看來「切勿點選不明附件檔案」的古老教訓依然適用。

而且，進一步的分析顯示，透過電子郵件散佈的惡意程式有 39.1% 是透過指向惡意程式碼的超連結，而非使用含有惡意程式的附件。這項數字比 2010 的 23.7% 上升了不少，這也進一步顯示網路罪犯正嘗試改變攻擊管道 (從純電子郵件轉向採用網頁) 來躲避資訊安全措施。

圖 14

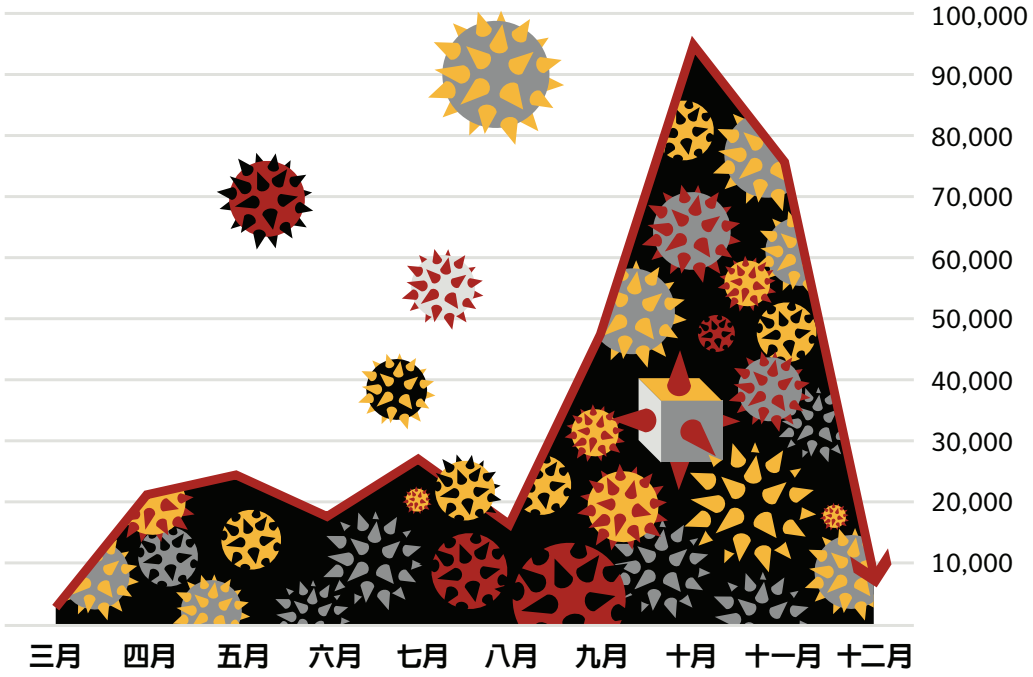
2011 年電子郵件當中的惡意程式比率



資料來源：賽門鐵克雲端服務

圖 15

2011 年透過電子郵件散佈的 Bredolab 變形惡意程式攻擊每月增加數量



資料來源：賽門鐵克雲端服務

邊界閘道通訊協定 (BGP) 挾持

2011 年，我們調查了[註 34]一個案例，一家俄羅斯的電信業者，其網路遭到垃圾郵件作者挾持。歹徒利用「邊界閘道通訊協定 (Border Gateway Protocol，簡稱 BGP)」這項網際網路基礎技術來散佈看似來自正常來源的垃圾郵件。由於垃圾郵件過濾技術有一部分是靠已知垃圾郵件來源黑名單來運作，因而讓這項技巧能躲過偵查。在該年當中，我們發現好幾個像這樣的案例。即使目前這樣的案例相較於大型傀儡網路所散發的垃圾郵件來說算是少數，但卻是未來一年值得觀察的重點之一。

變形威脅

變形惡意程式，或者更精確的說，「伺服器端」變形技術，是惡意程式作者與資訊安全廠商裝備競賽當中的最新高等技巧。所謂的變形技巧就是不斷改變惡意程式的內部結構或內容。這讓傳統的特徵比對惡意程式防護技術更難偵測。例如，如果在網站伺服器或雲端上執行這項技巧，攻擊者就能針對每一次攻擊產生一個獨特的惡意程式版本。

在 2011 年當中，賽門鐵克雲端服務電子郵件掃描程式經常、且大量發現 Trojan.Bredolab 變形威脅。此惡意程式佔所有電子郵件惡意程式攔截數量的 7.5%，約等於一整年有 3,500 萬次潛在攻擊。它採用了多種匿蹤的技巧，包括：伺服器端變形技巧、客製化包裝程式以及加密通訊。圖 15 顯示雲端式技術所發現的 Bredolab 變形惡意程式威脅增加數量變化。此圖顯示偵測到含有附件檔案偽裝成發票或收據以引誘收件人開啓的電子郵件數量。

危險網站

圖 16

2011 年最危險的網站類別

排名	最常遭受攻擊的前十大網站類型	佔所有受感染網站的百分比
1	部落格/網頁通訊	19.8%
2	託管/個人託管網站	15.6%
3	商業/經濟	10.0%
4	購物	7.7%
5	教育及參考	6.9%
6	科技、電腦及網際網路	6.9%
7	娛樂及音樂	3.8%
8	汽車	3.8%
9	健康與藥品	2.7%
10	色情圖片	2.4%

資料來源：賽門鐵克

透過網頁發動攻擊：攻擊工具組、Rootkit 及社交網路威脅

攻擊工具組可讓歹徒不必從頭撰寫軟體就能輕鬆開發新的惡意程式並策劃整個攻擊行動，這幾乎佔了惡意網站上所有威脅活動的三分之二 (61%)。隨著這類工具組愈來愈普遍、成熟、且更容易使用，此數字將繼續攀升。新的漏洞攻擊很快就能整合到攻擊工具組當中。該年當中，每一個新釋出的工具組版本，都增加了不少惡意的網頁攻擊活動。隨著新版本的推出與新漏洞攻擊功能的整合，我們發現工具組的使用情況愈來愈普遍，並且會將新的漏洞攻擊發揮到淋漓盡致，直到受害者修補系統為止。舉例來說，**2010** 年非常活躍的 **Blackhole** 工具組，其攻擊數量到了 **2011** 年中期只剩下每天幾百次，但是當其再度推出新版本之後，截至年底之前，每天都可以發現數十萬次的嘗試感染攻擊。

平均來說，一個攻擊工具組大約包含 10 個不同的漏洞攻擊，絕大多數都集中在不限特定瀏覽器的外掛程式漏洞，如：Adobe Flash Player、Adobe Reader 及 Java。熱門的工具組每幾天就會更新一次，而每次更新就會引發一波全新的攻擊。

它們在網路上很容易找到，而且在地下黑市和網站論壇上都有販售，價格從 **40** 至 **4,000** 美元不等。

網頁攻擊工具組對攻擊者的主要用途有二：

1. **目標式攻擊**。攻擊者先選定要攻擊的使用者類型。使用工具組建立用來引誘目標對象上當的電子郵件、即時通訊、部落格文章。這通常是一個指向惡意網站的連結，該網站會在受害者的系統上安裝惡意程式。

2. **大範圍**攻擊。攻擊者先利用 SQL 溢注、網頁軟體或伺服器漏洞來攻擊一大批網站。其目的是要從已感染的網站插入一個連結到另一個網站，讓該網站成為可以感染瀏覽者的惡意網站。一旦成功，接下來的每一位瀏覽者都會遭到攻擊。

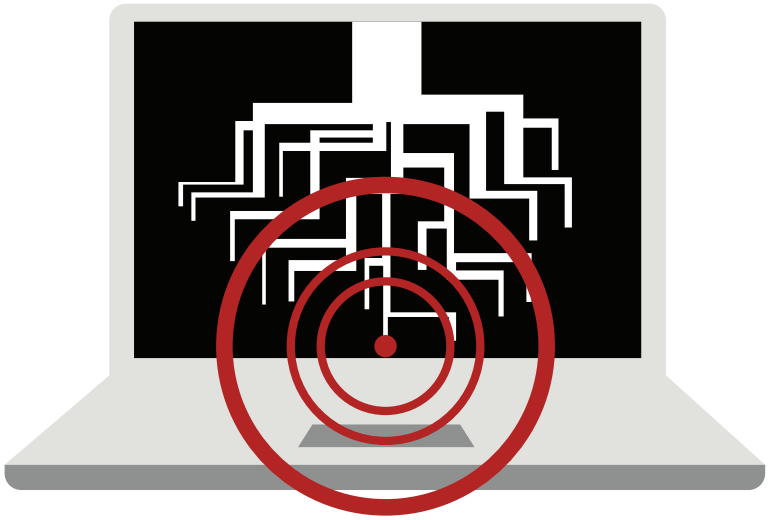
Mac 電腦也無法倖免

目前所知第一個感染 Mac 電腦的傀儡網路出現於 2009 年，我們在 2011 年看到多種專門針對 Mac OS X 電腦的新威脅，包括一些木馬程式，如 MacDefender 這個假防毒軟體。它看起來很像真的，而且安裝時不需要系統管理員權限。Mac 使用者面臨了一些會透過 SEO 搜尋引擎毒化與社交網路在電腦植入木馬程式的威脅。2011 年 5 月，賽門鐵克發現了一個專為 Mac 設計的惡意程式工具組 (Weyland-Yutani BOT)，這是第一個專門攻擊 Mac OS X 平台的工具組，採用網站溢注為攻擊手法。雖然這類犯罪工具組在 Windows 平台上非常普遍，但這卻是第一套在外販售的 Mac 平台犯罪工具組[註 35]。此外，許多攻擊工具都已經具備跨平台能力，可攻擊 Mac 或 Windows 電腦上的 Java 漏洞。在這樣的趨勢之下，Mac 使用者必須更注意安全問題，千萬不能假設使用 Mac 就能自動對所有威脅免疫。

圖 17

Macdefender 木馬程式擷取畫面

資料來源：賽門鐵克



Rootkit

Rootkit 是一種藉由竄改作業系統功能來躲避系統管理員偵查，並且讓歹徒持續擁有系統管理員權限的程式。Rootkit 已存在多年，1986 年發現的 Brain 病毒是第一個在 PC 平台上使用這類技巧的 Rootkit 程式，自此，這類程式的精密度和複雜度就不斷提升。

Rootkit 只佔了所有攻擊的一小部分，但卻是一個逐漸值得關注的問題，因為它們可以躲在系統深處，而且很難偵測及移除。目前 Rootkit 領域的首要威脅是 Tidserv、Mebratix 與 Mebroot。這些程式都會修改 Windows 電腦的主開機磁區 (MBR)，因此可以在作業系統載入之前就取得控制權。一些 Downadup (亦稱 Conficker) 的變種、Zbot (亦稱 ZeuS)，以及 Stuxnet 也都在某種程度上使用了 Rootkit 技巧。

隨著惡意程式碼變得愈來愈精密，最後有可能會轉變成某種可以躲避偵測並防止遭到移除的 Rootkit 技巧。由於使用者對於專門竊取機密資訊的惡意程式碼愈來愈有警覺性，加上攻擊者之間的競爭也持續升高，未來有可能會有更多威脅加入 Rootkit 的技巧來躲避資訊安全軟體。

社交媒體威脅

社交網站上聚集了數以億計的人口，無可避免地也會引來網路罪犯。社交媒體非常有利於施展社交工程技巧，因為當人們以為自己身邊圍繞的都是好友時，就很容易受騙上當。社交網站上所發現的攻擊有半數以上都是透過遭入侵的部落格/網頁通訊網站。因為，這些已遭入侵的網站連結經常在社交網路上轉貼。同樣地，愈來愈多的垃圾訊息也都利用社交網路來散發。

所有社交媒體平台都會遭到各種不同的攻擊。不過由於 Facebook 最受歡迎，因此提供了許多社交工程技巧如何在社交媒體上蓬勃發展的最佳範例。歹徒專門利用人們的需求和預期心理。例如，Facebook 不提供按「不讚」的按鈕，也不提供讓使用者看看自己有多少追隨者的功能，因此，歹徒就專門利用人們這樣的需求心理。

消除漏洞的空窗期：漏洞攻擊與零時差攻擊

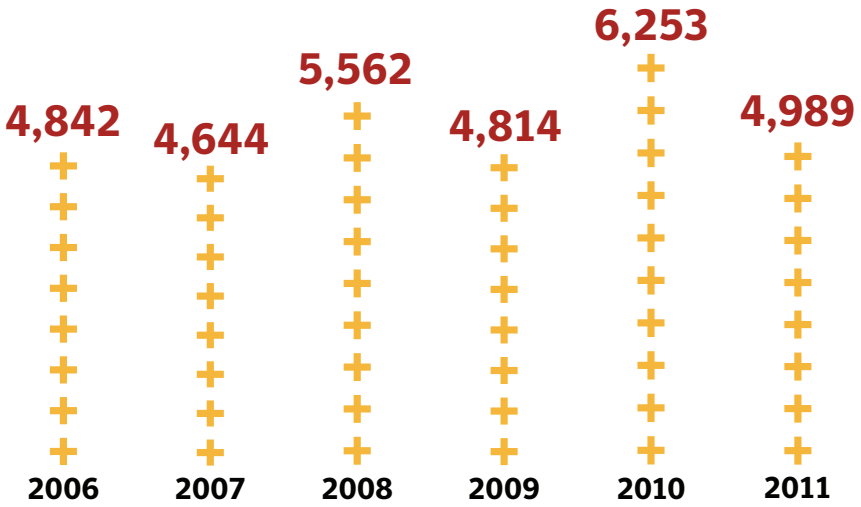
漏洞數量

我們在 2011 年發現 4,989 個新的漏洞，而前一年則為 6,253 個。(參見「附錄 D」來查看歷史資料以及我們調查方法的細節。)儘管數量減少，長期的整體趨勢依舊是上揚，而且賽門鐵克每星期都大約發現 95 個新的漏洞。

所謂的漏洞就是一種軟體上的「弱點」，例如程式撰寫的錯誤或設計缺失，讓攻擊者能夠利用它來破壞電腦系統的可用性、機密性或一致性。及早偵測並盡責通報，有助於降低漏洞在修補之前遭人利用的風險。

圖 18

2006-2011 年發現的漏洞總數



資料來源：賽門鐵克

重大基礎建設系統的弱點

監督控制與資料擷取 (Supervisory Control and Data Acquisition，簡稱 SCADA) 系統廣泛應用在工業與基礎建設產業，例如：發電廠的監控系統。我們發現公開通報的 SCADA 漏洞急速增加，從 2010 年的 15 個竄升至 2011 年的 129 個。自從 Stuxnet 病蟲在 2010 年 [註 36] 出現以來，SCADA 系統就受到資訊安全研究人員更大的關注。然而，新公告的 129 個漏洞當中卻有 93 個都是同一位研究人員的成果。

舊的漏洞仍舊遭到攻擊

PC 上有一個六年前發現的 Microsoft 作業系統舊漏洞 [註 37] 至今仍是 2011 年最常遭到攻擊的漏洞：這個 Windows RPC 元件漏洞 [註 38] 吸引了 6,100 萬次的攻擊。它所受到的攻擊次數，比排行在它後面的四個漏洞所受的總攻擊次數加起來還多 [註 39]。

PDF 是 2011 年最常被利用的資料檔格式。舉例來說，有一個 PDF 漏洞在 2011 年就吸引了超過一百萬次的攻擊。

最常遭到攻擊的前五大漏洞都已有修補程式，但為何歹徒還是會鎖定這些漏洞？這有幾點原因。

1. 攻擊這些漏洞的成本較低。歹徒必須在黑市上付出高額的代價[註 40]才能獲得有關新漏洞的情報，但他們只要購買現成的惡意程式就能攻擊舊的漏洞。
2. 攻擊較新的漏洞可能會比攻擊廣為人知的舊漏洞更容易引起注意。有些網路罪犯比較喜歡低調一點。
3. 外面仍有廣大的潛在受害者可供攻擊，因為有些使用者不能、不會或根本不安裝修補程式，也不安裝最新的主動式端點安全產品。

網頁瀏覽器漏洞

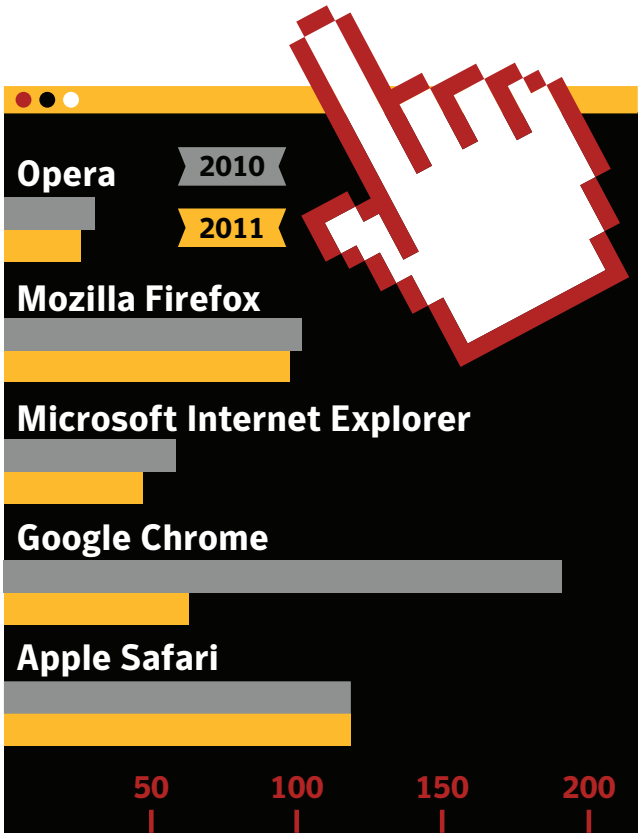
網頁瀏覽器是歹徒熱門的攻擊目標之一，他們會利用 Internet Explorer、Firefox、Chrome 等瀏覽器的漏洞，也會利用其外掛程式的漏洞，如 PDF 閱讀器。歹徒只要花 100 至 1,000 美元就能買到可在使用者瀏覽已感染網站時攻擊高達 25 項不同漏洞的工具組。

在 2011 年當中，我們看到所有熱門瀏覽器的通報漏洞數量都大幅減少，從 2010 年的 500 個下降至 2011 年的 351 個。其中，有很大一部分的原因是 Google Chrome 漏洞數量大幅減少。

不過，瀏覽器外掛程式的整體漏洞數量只減少了一點點，從 346 下降至 308 個。

圖 19

2010 及 2011 年瀏覽器漏洞



資料來源：賽門鐵克

新的零時差漏洞造成重大危險

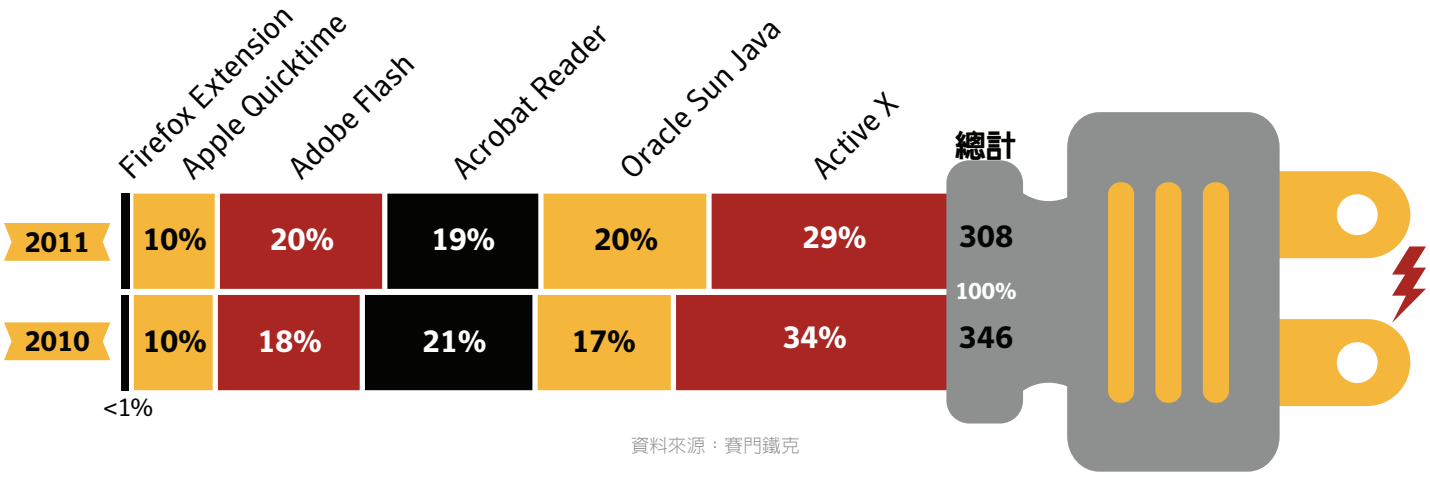
所謂的零時差（zero-day）攻擊，就是使用尚未通報的漏洞，因此沒有任何廠商可提供修補程式。所以，這類漏洞特別危險，因為攻擊的成功機率大增。如果某個已通報的漏洞攻擊越過了資訊安全防線，只要軟體已完成修補就不會遭到危害。但若遇到零時差攻擊可就沒轍。

例如，在 2011 年當中，我們看到 Adobe Reader 和 Adobe Acrobat 的某個漏洞[註 41]遭到了嚴厲的攻擊，並且持續了二個星期以上。在 2011 年 12 月 16 日 Adobe 釋出修正程式之前，最高每天有 500 次以上的攻擊。

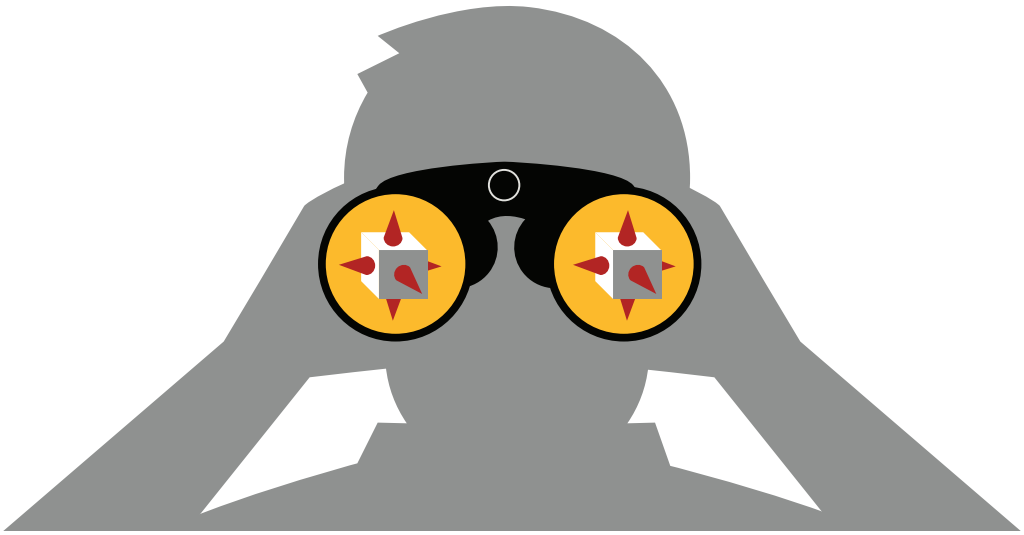
好消息是，2011 年是過去 6 年來零時差漏洞最少的一年。儘管零時差漏洞的整體數量下降，但使用這類漏洞的攻擊還是相當成功，這也是為何目標式攻擊經常使用這類漏洞，例如：W32.Duqu。

圖 20

瀏覽器外掛程式漏洞



資料來源：賽門鐵克



結論：
展望 2012 年

智者常言：「不要預測，尤其不要預測未來。」但這份報告已經回顧了 2011 年的整體情勢，我們不免要在結論當中稍微展望一下未來，並且推測 2012 年以及更遠的趨勢。

目標式攻擊與進階持續性攻擊威脅 **(APT)** 將繼續成為一項嚴重問題，而且這類攻擊的頻率和複雜度也將提高。

目標式攻擊所運用的技巧和漏洞攻擊，也將下放至地下經濟體系當中的廣大族群，因此一般的惡意程式將更加危險。

惡意程式和垃圾郵件作者將更加善用社交網站。

CA/Browser Forum (憑證核發機構/瀏覽器論壇)[註 42] 將釋出更多有關憑證核發機構的安全規範，以確保網際網路信任體系的安全，防範未來可能的攻擊。

IT 消費化與雲端運算將持續演進，可能因此改變商業運作模式，迫使 **IT** 部門開始轉型並尋找新的方法來保護一般使用者及企業系統。

惡意程式作者也將繼續發掘新的手法來攻擊手機和平板電腦等行動裝置，而且，只要他們發現任何有效的賺錢方式，他們一定會毫不留情地發揮到極致。

2011 年，針對 **Mac** 平台的惡意程式碼開始比以前更多，**Mac** 使用者開始面臨會在系統植入木馬程式的惡意網站。預料此趨勢將延續至 **2012** 年，因為針對 **Mac** 漏洞的攻擊程式碼也將與更廣泛的網頁攻擊工具組進一步整合。

雖然外部威脅將持續增加，但內賊的威脅 **(**員工蓄意或非蓄意的資料外洩或竊取行為**)** 同樣也會讓公司登上報紙頭條。

下一個類似 **Stuxnet** 的 **APT** 攻擊或許已經佈下了基礎。的確，**Duqu** 或許預告了全新一波震撼的開始，但餘震或許還要等一陣子才會到來。

給企業的最佳實務準則

採用縱深防禦的策略：

強化多重、重疊、彼此互相支援的防禦系統來防止任何特定技術或防護方法的單一故障點。這應包括在整個網路上部署常態更新的防火牆、閘道防毒、入侵偵測、入侵防護等系統，還有網頁安全閘道解決方案。

監控網路威脅、漏洞與品牌是否遭到濫用。

監控網路入侵、散播及其他可疑的流量模式，發掘連上已知惡意或可疑主機的連線。接收所有廠商平台的最新漏洞與威脅警示，主動加以矯正。透過網域警示與假網站通報追蹤品牌是否遭到濫用。

光有端點裝置防毒是不夠的：

光有端點裝置上的特徵式防毒，並不足以對抗今日的威脅和網頁式攻擊工具組。務必部署並使用一套內含下列額外防護的完整端點安全產品：

- 端點入侵預防 — 防止未修補的漏洞遭到攻擊，防止社交工程攻擊，防止惡意程式進入端點裝置。
- 瀏覽器防護 — 防止偽裝的網頁式攻擊。
- 考慮採用雲端式惡意程式防護，主動防範未知威脅。
- 檔案和網頁式信譽解決方案 — 提供任何應用程式及網站的風險與信譽評等，預防快速變種與變形的惡意程式。
- 行為式預防能力 — 查看應用程式和惡意程式的行為以預防惡意程式。
- 應用程式控管設定 — 預防應用程式和瀏覽器外掛程式下載未經授權的惡意內容。
- 裝置控管設定 — 預防並限制可用的 USB 裝置類型。

保護您的網站，防止 MITM 攻擊與惡意程式感染：

透過下列方式避免您與客戶之間的信任關係破裂：

- 採用 Always On SSL (全程啓用 SSL)。
- 每天定期掃描您的網站是否有惡意程式。
- 為所有的連線階段 cookie 設定安全旗標。
- 定期檢查您的網站是否有漏洞。
- 採用強化驗證的 SSL 憑證 (EV SSL)，如此一來，瀏覽器會顯示綠色底色的網址列來告知網站使用者。
- 在網站上的醒目位置顯示知名信任標章，讓使用者瞭解您在安全上的用心，提升信賴感。

務必從知名、值得信賴、且具有良好安全措施保護的憑證核發機構取得您的數位憑證。**妥善保護您的私密金鑰：實施嚴格的安全實務來保護您的私密金鑰，尤其若您有在使用數位憑證的話。**賽門鐵克建議企業應該：

- 使用分開的「測試簽署與發行簽署 (Test Signing and Release Signing)」基礎架構。
- 將金鑰儲存在安全、無法竄改、加密的硬體裝置。
- 建置實體安全措施來保護您的資產以防止竊盜。

使用加密來保護敏感資料：

建立並強制執行安全政策，規定敏感資料必須加密。存取敏感的資訊應該受到管制，包括使用一套可發掘、監控及保護資料的防止資料外洩 (Data Loss Protection，DLP) 解決方案。這不僅可以預防資料外洩，也可以降低資料從企業內部外流的潛在損失。

使用防止資料外洩技術來預防資料外流：

建置一套 DLP 解決方案來發掘敏感資料所在位置、監控這些資料的使用，並且防止這些資料外流。DLP 應該用來監控透過網路傳送至企業外部的資料，此外也要監控複製到外接裝置或網站的敏感資料。DLP 應設定攔截可疑的敏感資料複製或下載行為。同時，DLP 也應用來發掘網路檔案系統與個人電腦上的機密或敏感資料，如此才能藉由適當的資料保護措施 (如加密) 來降低資料外洩的風險。

制定一套抽取式媒體管制政策。

如果可行的話，禁止使用非經授權的裝置，例如：外接行動硬碟與其他抽取式媒體。這類裝置不僅可能帶來惡意程式，更可能導致智慧財產 (蓄意或非蓄意) 外流。如果您准許使用外接媒體裝置，則在裝置連上網路時自動執行掃毒，並且利用 DLP 解決方案來監控並禁止機密資料複製到非加密的外接儲存裝置。

經常且迅速更新您的安全防護措施：

有鑑於賽門鐵克在 2011 年發現了 4 億零 3 百萬個非重複的惡意程式變種，企業應該至少每天更新一次病毒與入侵預防定義檔，可能的話最好一天更新數次。

積極更新及修補：

透過廠商的自動更新機制來更新、修補並升級過時且不安全的瀏覽器、應用程式及瀏覽器外掛程式，使用最新可用的版本。大多數的軟體廠商都會積極修補軟體漏洞，但這些修補程式也得套用了才能發揮作用。在部署含有舊版瀏覽器、應用程式及瀏覽器外掛程式的企業標準系統影像時要特別小心，這些程式很可能已經過時而不安全。盡可能將修補程式部署自動化，讓整個企業都能隨時免於漏洞攻擊。

強制執行有效的密碼政策。

確保密碼強度足夠，密碼至少要 8 至 10 個字元，而且應混合字母和數字。鼓勵使用者避免在不同網站重複使用相同的密碼，而且應嚴格禁止與他人共用密碼。密碼應定期更換，至少 90 天更換一次。切勿將密碼寫下來。

限制使用電子郵件附件檔案：

設定電子郵件伺服器攔截並移除含有病毒常用附件檔案的電子郵件，如：**.VBS**、**.BAT**、**.EXE**、**.PIF** 及 .SCR 檔案。企業應仔細研究哪些 .PDF 檔案可以當成電子郵件附件。

確實建立惡意程式感染與事件回應程序：

確實保管您資訊安全廠商的連絡資訊，瞭解萬一系統遭到感染時該連絡誰、該採取什麼步驟。

確實建置一套備份復原解決方案，以便萬一遭到攻擊或發生災難而遺失資料時，可以復原遺失或損毀的資料。

利用網頁閘道、端點安全產品及防火牆的感染後偵測功能來發掘遭到感染的系統。

隔離已感染的電腦，防止企業內部進一步遭到感染的風險。

如果網路服務遭到惡意程式碼或其他威脅攻擊，關閉這些服務，直到套用修補程式為止。

對任何遭感染的電腦進行鑑識分析，使用可信任的媒體將這些電腦復原。

教育使用者有關最新的威脅情勢變化：

切勿開啓附件檔案，除非是預期的檔案且來自已知可信任的來源，而且切勿執行網際網路上下載的軟體 (如果公司允許的話)，除非下載檔案已經過病毒掃描。

在點選電子郵件或社交媒體上的連結時要小心，即使來自可信任的來源和好友也一樣。

切勿貿然點選縮短網址，務必先使用一些工具或外掛程式來預覽或將它展開查看。

建議使用者要留意自己在社交網路上公開的資訊，因為這些資訊可能被歹徒用於鎖定他們或引誘他們開啓惡意的網址或附件檔案。

小心搜尋引擎所列出的查詢結果，並且只點選可信任的資料來源，尤其是媒體上的熱門話題。

安裝可在搜尋結果上顯示網站信譽評等的網頁瀏覽器外掛程式。

只從公司內部分享來源或廠商的網站下載軟體 (如果公司允許的話)。

如果 Windows 使用者在點選某個連結或搜尋引擎結果時看到一個宣稱使用者「已遭感染」的警告訊息，請使用者利用 Alt-F4、CTRL+W 或「工作管理員」來關閉瀏覽器。

建議使用者使用最新的瀏覽器與作業系統，並且隨時將系統更新至最安全的狀態。

教育使用者在登入網站或在網站上分享任何個人資料時，要看看瀏覽器上是否在網址列顯示綠色底色、HTTPS 字樣，或是網站上是否有信任標章。

給消費者的最佳實務準則

保護自己：

使用含有下列功能的最新網際網路安全軟體，以提供最大的惡意程式碼與其他威脅防護：

檔案特徵式與啓發式防毒與惡意程式行為預防 — 防止未知惡意威脅執行。

雙向防火牆 — 防止惡意程式攻擊您電腦上可能含有漏洞的應用程式與服務。

入侵預防 — 防止網頁攻擊工具組、未修補的漏洞以及社交工程攻擊。

瀏覽器防護 — 防止偽裝的網頁式攻擊。

信譽式工具 — 可在下載之前先檢查檔案和網站的信譽和可信度；提供搜尋結果顯示的 URL 信譽和網站的安全評等。

考慮採用跨平台的家長監護功能，例如：諾頓家長防護網 (Norton Online Family) [註 43]。

保持更新：

隨時更新病毒定義檔與安全內容，如果無法每小時更新，至少每天更新一次。安裝最新的病毒定義檔，讓您的電腦能夠防止已知在外流傳的最新病毒與惡意程式。透過內建的自動更新功能 (若有) 來更新您的作業系統、網頁瀏覽器、瀏覽器外掛程式及應用程式至最新版本。執行過時的版本會讓您處於網頁式攻擊的風險當中。

知道自己在做什麼：

請注意，那些千方百計想要讓您誤以為自己的電腦遭到感染的惡意程式或應用程式，很可能是在您安裝檔案分享程式、免費下載、免費軟體或共享軟體時一併自動安裝的。

「免費」、「破解」或「盜版」的軟體可能會挾帶惡意程式，或者含有讓您誤以為電腦遭到感染而被迫付費來清除的社交工程攻擊。

小心挑選自己所瀏覽的網站。當然，惡意程式也可能來自於主流網站，但一些提供免費色情內容、賭博或盜版軟體的網站，更可能挾帶惡意程式。

看到終端用戶授權協議 (EULA) 畫面時，請仔細閱讀並瞭解其內容，因為有時候某些資訊安全風險就是在您接受協議之後或者因為您自願接受才安裝的。

採用有效的密碼政策：

務必使用混合字母和數字的密碼，並且經常更換。密碼當中不應含有字典中的字。切勿多個應用程式或網站都使用相同密碼。使用複雜的密碼 (包括大小寫和標點符號)。

點選之前請三思：

千萬別貿然檢視、開啓或執行任何電子郵件當中的附件檔案，除非您預期會收到，而且您信任寄件者。即使是來自於可信任的使用者，還是要保持警戒。

在點選電子郵件或社交媒體上的連結時要小心，即使來自可信任的來源和好友也一樣。切勿貿然點選縮短網址，務必先透過預覽或外掛程式來將它展開查看。

切勿在社交網站上點選標題或詞句聳動的連結，即使來自好友也一樣。萬一您點選了網址，您可能因此莫明其妙地按了一個「讚」，並且發送給所有的好友，即使您按的是網頁上的隨意位置也一樣。此時請關閉或離開瀏覽器。

請使用可在搜尋結果上顯示網站信譽評等的網頁瀏覽器外掛程式。小心搜尋引擎所列出的查詢結果，並且只點選可信任的資料來源，尤其是媒體上的熱門話題。

小心那些要求您安裝媒體播放程式、文件閱讀器及安全更新的彈出式訊息，請直接從廠商的網站下載軟體。

守護您的個人資料：

盡可能減少您在網際網路上公開的個人資訊，包括 (尤其是) 透過社交網路，因為這可能會遭有心人士收集並用於惡意活動，例如：目標式攻擊和網路釣魚詐騙。

切勿公開任何機密的個人或財務資訊，除非您確定這類要求合理。

經常檢查您的銀行、信用卡帳單和信用狀況，看看是否出現異常活動。避免從公共電腦 (如圖書管、網咖等等) 或者透過未加密的 Wi-Fi 網路連上網路銀行或在線上購物。

當透過 Wi-Fi 網路連線登入電子郵件、社交媒體和分享網站時，請使用 HTTPS 加密連線。檢查您所使用的應用程式和網站的設定和偏好設定。

當您在網站上登入或提供任何個人資訊時，檢查一下瀏覽器網址列是否有綠色底色、**HTTPS 字樣或者網站上有可辨認的信任標章**。

設定您家中的 **Wi-Fi 網路使用嚴格的驗證**，並且務必使用密碼才能連線。

更多資訊

賽門鐵克雲端服務 全球威脅：http://www.symanteccloud.com/en/gb/globalthreats/

賽門鐵克安全機制應變中心：http://www.symantec.com/security_response/

網路安全威脅研究報告資源頁面：http://www.symantec.com/threatreport/

諾頓 Threat Explorer：http://us.norton.com/security_response/threatexplorer/

諾頓網路犯罪索引：http://us.norton.com/cybercrimeindex/

關於賽門鐵克

賽門鐵克為資訊安全、儲存與系統管理解決方案之全球領導者，協助消費者和企業保護與管理以資訊為導向的世界。我們的軟體與服務能夠以更完整、更有效率的方式，在更多的端點避免更多的風險，無論資訊使用與存放的地點為何，都能讓您充滿信心。賽門鐵克總部位於美國加州 Mountain View 市，在 40 個國家設有營運據點。欲知更多資訊，請上網查詢：www.symantec.com。

附註

1 請注意。這項數據首次包含來自賽門鐵克雲端服務的資料。若去掉這些數據再與 2010 年的數據比較，則攻擊總數將為 51 億次。

2 Gartner 於 2011 年 11 月 8 日發表之新聞稿，「Gartner Says Consumerization Will Drive At Least Four Mobile Management Styles (Gartner 指出消費化將帶來至少四種行動裝置管理風格)」。http://www.gartner.com/it/page.jsp?id=1842615

3 https://otalliance.org/resources/AOSSL/index.html

4 http://www.nortoncybercrimeindex.com/

5 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

6 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

7 http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_UK_Cyber_Security_Strategy.pdf

8 http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011

9 Ponemon Institute 於 2012 年 3 月發表之「2011 Cost of Data Breach Study: United Kingdom (2011 年資料外洩成本研究：英國)」。

10 2011 年憑證核發機構遭駭 (Comodohacker)、資料外洩與憑證徹銷：Comodo (2 家 RA 遭駭)：https://www-secure.symantec.com/connect/blogs/how-avoid-fraudulent-ssl, http://www.thetechherald.com/articles/InstantSSL-it-named-as-source-of-Comodo-breach-by-attacker/13145/

11 http://www.theregister.co.uk/2011/05/24/comodo_reseller_hacked/

12 StartCom 遭到攻擊。http://www.internet-security.ca/internet-security-news-archives-031/security-firm-start-ssl-suffered-a-security-attack.html, http://www.informationweek.com/news/security/attacks/231601037

13 http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/

14 DigiNotar 因資料外洩而倒閉。https://www-secure.symantec.com/connect/blogs/why-your-ca-matters, https://www-secure.symantec.com/connect/blogs/diginotar-ssl-breach-update , http://www.arnnet.com.au/article/399812/comodo_hacker_claims_credit_diginotar_attack/, http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars, http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231600865/comodo-hacker-takes-credit-for-massive-diginotar-hack.html http://www.pcworld.com/businesscenter/article/239534/comodo_hacker_claims_credit_for_diginotar_attack.html

15 攻擊與學術概念驗證示範：BEAST (http://blog.ivanristic.com/2011/10/mitigating-the-beast-attack-on-tls.html) 與 TLS 1.1/1.2、THC-SSL-DOS、LinkedIn SSL Cookie 漏洞 (http://www.wtfuzz.com/blogs/linkedin-ssl-cookie-vulnerability/)、

16 http://www.itproportal.com/2011/09/13/globalsign-hack-was-isolated-server-business-resumes/

17 http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/

18 http://www.pcworld.com/businesscenter/article/239639/dutch_government_struggles_to_deal_with_diginotar_hack.html

19 http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/

20 https://otalliance.org/resources/AOSSL/index.html

21 http://blog.facebook.com/blog.php?post=486790652130

22 http://blog.twitter.com/2011/03/making-twitter-more-secure-https.html

23 http://www.symantec.com/connect/blogs/launch-always-ssl-and-firesheep-attacks-page

24 由賽門鐵克所贊助，於 2010 年 12 月與 2011 年 1 月在英國、法國、德國、比荷盧、美國及澳洲等地進行的網際網路購

物者消費調查 (研究於 2011 年 3 月執行)。

25 http://www.symantec.com/about/news/release/article.jsp?prid=20111129_01

26 http://www.symantec.com/connect/blogs/protecting-digital-certificates-everyone-s-responsibility/

27 http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport

28 http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/

29 「AMD 2011 Global Cloud Computing Adoption, Attitudes and Approaches Study (AMD 之 2011 年全球雲端運算接受度、態度與方法研究)」http://www.slideshare.net/AMDUnprocessed/amd-cloud-adoption-approaches-and-attitudes-research-report

30 附錄 C：垃圾郵件與詐騙活動趨勢

31 http://www.symanteccloud.com/en/gb/mlireport/MLI_2011_05_May_FINAL-en.pdf

32 欲知更多有關諾頓網頁安全資訊，請造訪以下網站：http://safeweb.norton.com

33 欲知更多有關賽門鐵克網站漏洞評估服務資訊，請造訪以下網站：http://www.symantec.com/theme.jsp?themeid=ssl-resources

34 如需附錄 C 中的進一步資訊，請參考：垃圾郵件與詐騙活動趨勢

35 http://krebsonsecurity.com/tag/weyland-yutani-bot/

36 欲知更多關於 Stuxnet 的資訊，請參考：http://www.symantec.com/connect/blogs/hackers-behind-stuxnet 和 http://www.youtube.com/watch?v=cf0jIzVCyOI

37 CVE-2008-4250 請參考：http://www.securityfocus.com/bid/31874

38 2011 年發現了 6,120 萬次針對 Microsoft Windows RPC 元件的攻擊，而且大部分是利用 Microsoft Windows 伺服器服務 RPC 處理方式會允許遠端程式碼執行的漏洞 (BID 31874)。請參考：http://www.securityfocus.com/bid/31874

39 附錄 D：漏洞趨勢：圖 D.3

40 請參考：http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/231900575/more-exploits-for-sale-means-better-security.html

41 CVE-2011-2462 請參考 Adobe Security Advisory：http://www.adobe.com/support/security/advisories/apsa11-04.html。

42 於 2011 年 12 月 1 日至 2011 年 12 月 16 日得自賽門鐵克雲端服務之攻擊大量資料。

43 http://www.cabforum.org/

44 欲知更多有關諾頓家長防護網資訊，請造訪以下網站：https://onlinefamily.norton.com/

關於賽門鐵克

賽門鐵克為資訊安全、儲存與系統管理解決方案之全球領導者，協助消費者和企業保護與管理以資訊為導向的世界。我們的軟體與服務能夠以更完整、更有效率的方式，在更多的端點避免更多的風險，無論資訊使用與存放的地點為何，都能讓您充滿信心。賽門鐵克總部位於美國加州 Mountain View 市，在 40 個國家設有營運據點。如需更多詳細資訊，請造訪：www.symantec.com。

若您需要任何一個分公司的聯絡電話或相關資訊，請造訪我們的網站。

如需產品資訊，請上網查詢。美國地區客戶請洽免付費電話：1 (800) 745 6054。

台灣賽門鐵克股份有限公司

地址：台北市 105 南京東路五段 188 號 2F-7

電話：(02) 8761-5800

傳真：(02) 2742-2838

www.symantec.com.tw

2012 年 4 月出刊